DISCUSSION PAPER SERIES

No. 4509

DEFENCE R&D IN THE ANTI-TERRORIST ERA

Manuel Trajtenberg

INDUSTRIAL ORGANIZATION

Centre for Economic Policy Research

www.cepr.org

Available online at: **www.cepr.org/pubs/dps/DP4509.asp**

ISSN 0265-8003

DEFENCE R&D IN THE ANTI-TERRORIST ERA

Manuel Trajtenberg, Tel Aviv University and CEPR

Discussion Paper No. 4509
July 2004

Centre for Economic Policy Research
90–98 Goswell Rd, London EC1V 7RR, UK
Tel: (44 20) 7878 2900, Fax: (44 20) 7878 2999
Email: cepr@cepr.org, Website: www.cepr.org

CEPR Discussion Paper No. 4509

July 2004

ABSTRACT

Defence R&D in the Anti-Terrorist Era*

This Paper seeks to analyse the nature of the terrorist threat following 9/11, and to explore the implications for defence R&D policy. First, it reviews the defining trends of defence R&D since the Cold War, and brings in pertinent empirical evidence: the US accumulated during the 1990s a defence R&D stock 10 times larger than any other country, and almost 30 times larger than Russia. Big weapon systems, key during the Cold War but of dubious significance since then still figure prominently, commanding 30% of current defence R&D spending, versus just about 13% for intelligence and anti-terrorism. The second part of the Paper examines the nature of the terrorist threat, focusing on the role of uncertainty, the lack of deterrence, and the extent to which security against terrorism is (still) a public good. I develop for that purpose a simple model of terrorism, cast in a nested discrete choice framework. Two strategies are considered: fighting terrorism at its source, and protecting individual targets, which entails a negative externality. Contrary to the traditional case of national defence, security against terrorism becomes a mixed private/public good. A key result of the model is that the government should spend enough on fighting terrorism at its source, so as to nullify the incentives of private targets to invest in their own security. Intelligence emerges as the key aspect of the war against terrorism and, accordingly, R&D aimed at providing advanced technological means for intelligence is viewed as the cornerstone of defence R&D. This entails developing computerized sensory interfaces, and increasing the ability to analyse vast amounts of data. Both have direct civilian applications, and therefore the required R&D is mostly ‘dual use’. Indeed, there is already a private market for these systems, with a large number of players. R&D programmes designed to preserve this diversity and to encourage further competition may prove beneficial both for the required R&D, and for the economy at large.

JEL Classification: H40, H56 and O30
Keywords: defence R&D, dual-use, intelligence, public goods and terrorism

Manuel Trajtenberg
The Eitan Berglas School of
Economics
Tel-Aviv University
Tel-Aviv 69978
ISRAEL
Tel: (972 3) 640 9911
Fax: (972 3) 640 9908
Email: manuel@post.tau.ac.il

A shorter version of this Paper was presented at the NBER conference on 'Innovation Policy and the Economy', Washington, April 15, 2003. I am thankful to Alon Eisenberg and to Marina Tsirulnik for excellent research assistantship, to Guy Kaplan for helping with his military expertise, and to Jacob Glazer, Dan Peled, Oren Setter and Nadine Baudot-Trajtenberg for useful comments.

Submitted 21 June 2004

I. Introduction

The devastating terrorist attacks of 9/11 and their aftermath pose a formidable challenge to US national security, and call for the rethinking of established dogma in a wide range of fields. The attacks came after a relatively peaceful decade that constituted an interlude between the cold war, and the emerging terrorist threat. Defense R&D had proceeded over the post WWII decades along the familiar path of the arms race in the nuclear age, bounded only by treaties that sought to mitigate the spiraling costs and preserve the logic of the "mutually assured destruction" doctrine. This coincided with a golden era of scientific and technological progress,[1] unleashing extraordinary advances in military technology. The collapse of the Soviet Union, brought about in part by that same race, left the US as the only superpower, particularly in terms of its edge in military ***technology***. However, the new terrorist threat negated much of that advantage, since the enemy could neither be effectively deterred by overwhelming military force, nor could it be destroyed by actually deploying that force. In the meantime defense R&D continued by and large along the old path, still devoting large amount of resources to the development of big, complex, offensive weapon systems that have no rival in the world, and for which there is no clear threat that these costly weapons could forestall. A fresh look at defense R&D policy is thus called for, starting from a thorough analysis of the new terrorist threat and seeking to trace its implications for the required R&D. The main goal of this paper is to deploy some basic tools of economic analysis to this much-needed reassessment.

Section II characterizes in more detail defense R&D before 9/11, bringing data to bear both on the total stock of military R&D of the US *vis a vis* other leading countries, and on the composition of R&D spending. Simple computations of the defense R&D stock generated during the 1990s indicate that the US accumulated during that decade alone a stock 10 times as large as that of any other country, and almost 30 times larger than its old foe, Russia. Within this vast technological reservoir big weapon systems still figure prominently, commanding about 30% of current R&D spending (not including the

Ballistic Missile Defense program, which commands another 15%). On the other hand, R&D aimed at intelligence and antiterrorism, which the analysis below places at the forefront of the desirable defense R&D policy, constitute only about 13% of the known total.

Section III examines the nature of the terrorist threat, focusing on the role of uncertainty, the lack of deterrence, and the extent to which providing security against terrorism is still a public good. This later issue receives a more detailed treatment in section IV where I develop a simple model of terrorism, cast in a nested discrete choice framework. In its context one can analyze the probability that a terrorist attack will take place, and the (conditional) probability that any particular target will be hit. Two strategies are available to combat terrorism: The first consists of fighting terrorism at its source, thus reducing the overall probability that an attack will take place; this constitutes a public good and hence is to be provided by the government. The second entails potential targets investing in their own security, thus reducing the probability that they will be hit, but raising it for others (a negative externality). Contrary to the traditional case of national defense, the provision of security against terrorism thus becomes a mixed private/public good. A key result of the model is that the government should spend enough on fighting terrorism at its source, so as to nullify the incentives of private targets to invest in their own (local) security. The model allows also to explore the relative impact of R&D aimed at improving the effectiveness of spending on each type of strategy.

Section V attempts to draw implications for the design of a coherent defense R&D policy that would fit the changing nature of the threats facing the US, and in particular the characterization of the terrorist threat as discussed in previous sections. Intelligence (in the broad sense) emerges as the key aspect of the war against terrorism and, accordingly, R&D aimed at providing advanced technological means for improved intelligence is viewed as the cornerstone of defense R&D. *Basic* R&D for target-specific

[1] At the beginning of the cold war the share of GDP devoted to R&D was just 1.4% (in 1953), it raised rapidly during the late 1950s to over 2%, and it has fluctuated since within the 2.3-2.9% range (see NSF's

protection from terrorist threats, R&D to counter non-conventional threats, and cyber security are further important aspects of such policy.

Section VI looks into the technological directions implied by the required antiterrorist R&D, and the implications for competition in the relevant markets. The provision of advanced means for intelligence and for target protection entails emulating human sensory perceptions through computerized sensory interfaces, and increasing dramatically the ability to analyze in real time vast amounts of information. Both have clear and direct civilian applications, and therefore the required R&D is mostly "dual use". The development of big weapon systems during the cold war led to high concentration of both R&D and procurement into a few large corporations, conferring them a great deal of market power. By contrast, the development of sensory computer interfaces, Internet security, biological protection, and the like, entails an entirely different playfield: these systems are as said dual use, there is (also) a private market for them, and there exist already a large number of players that can partake in the required R&D. New R&D programs could be designed so as to preserve this much-needed diversity and to encourage further competition. Such programs may prove highly beneficial both for the required defense R&D and for the advanced sectors of the economy themselves, thus fostering economic growth. Section VII concludes with a summary of the principles upon which defense R&D policy for the antiterrorist era could be articulated.

II. Defense R&D: before and after 9/11[2]

Since the 1950's and up to the 1990's the predominant security threat facing the USA was of course that posed by the Soviet Union, a threat that lead to a relentless arms race. The main goal of the USA military was, accordingly, to deter the USSR from attacking the USA or its allies (primarily western Europe), and if attacked, to be able to defeat any combination of threatening states (i.e. those making the Warsaw pact).[3]

---

report at http://www.nsf.gov/sbe/srs/infbrief/nsf03307/start.htm#fig2).

[2] For an overview of the economics of defense R&D, see Lichtenberg (1995).

[3] A further goal was "containment" of the soviet influence around the world, but it is less clear how that goal influenced defense R&D.

Defense R&D thus had very clear goals to serve, there was a well-defined (leading) foe, and the rules of the game were also well defined, evolving rather slowly throughout the dynamic interaction with the USSR.[4] This lead to the building of a formidable defense R&D complex, including DARPA, federal labs (such as Livermore, Argonne, Oak Ridge), large private contractors (such as Lockheed, Grumman, Raytheon), research at major universities (such as MIT and Stanford), as well as the R&D performed at the various branches of the military themselves.

Throughout the second half of the 20th century this vast complex developed ever more powerful and accurate weapons, and in particular big weapon systems such as nuclear devices, intercontinental ballistic missiles, nuclear submarines, large carriers, high-performing aircraft (including jetfighters, large transport planes, combat and transport helicopters, stealth aircraft), and so forth.[5] The logic of the cold war, of the arms race, dictated to a large extent the direction of R&D: thus for example, the prevalent "MAD" (mutually assured destruction) doctrine necessitated the development of nuclear subs, that could survive and operate autonomously even after a devastating nuclear attack on mainland USA, and deliver a retaliatory blow on the enemy. Conversely, various treaties with the USSR limited the development of antiballistic missiles.[6]

Fortunately for all involved, the logic of the MAD doctrine worked well, and the immense arsenal of highly sophisticated and lethal weapons developed in the course of the cold war, and in particular the big weapon systems, remained for the most part unutilized. It would seem that never before in history a relentless arms race terminated without a major confrontation, essentially by the internal (but not unrelated) collapse of one of the contenders. However, the enormous R&D resources poured into the development of those weapon systems over decades did achieve their goal: to deter a

[4] See for example the various treaties restricting the development, testing and/or deployment of various weapon systems, such as ABM's.
[5] For example, in the early 1980s a full 75% of federal outlays on defense R&D went to missiles and aircraft, two of the main items in the category of "big weapon systems" (see Mowery and Rosenberg, 1989).
[6] Hence the lack at present of effective defensive systems against the missile threats posed by Iraq, Iran and North Korea (the "Patriot" system did not perform well during the 1991 Gulf war, and it remains to be seen if the newly developed Israeli "Arrow" system, or the improved Patriot will do better).

major armed conflict. In that sense the relative peace in which most of the world lived for half a century, certainly the American people, owes as much to defense R&D as to anything else.

The collapse of the USSR shattered the basic premises that had guided defense R&D, primarily in that there was no longer a foe having commensurable capabilities and racing for parity or supremacy. Thus, attention gradually shifted away from the prospect of an all out war, to regional conflicts in which the USA may have a stake, as well as to issues stemming largely from the dismembering of the Soviet Union, such as preventing nuclear leakage. A common denominator of these new challenges was that the mighty deterrence built over the decades of the cold war was no longer effective, if only because the USA could not conceivably resort to a nuclear strike against foes that did not pose a commensurable threat to the USA itself. Defense R&D was to serve then new goals such as the ability to fight simultaneously two regional conflicts (thus emphasizing rapid deployment, maintainability of equipment, etc.) and to minimize casualties in any confrontation (one of the legacies from the Vietnam war). Yet throughout the 1990s a big chunk of defense R&D was still devoted to big weapon systems, such as the development of new, high-performing and extremely expensive aircraft. Indeed, and perhaps not surprisingly, defense R&D exhibited a large degree of inertia, partly as a consequence of the fact that R&D expenses grow rapidly as a project moves forward from basic research towards development, testing and evaluation. Thus "legacy" projects that were conceived a decade or more earlier proceeded to absorb increasing R&D resources over time even though the need for them had virtually vanished.

Much as the fall of the Soviet Union over a decade earlier marked the closing of an era, 9/11 signified the beginning of a new one, dominated by the worldwide terrorist threat (see Hoge and Rose, 2002). Of course, large-scale terrorism against the USA did not start with the attack on the WTC: the devastating attack on the US marine barracks in Beirut in 1983, the attacks on the US embassies in Nairobi and in Dar e-Salaam in 1998, and the attack on the USS Cole in October 2000 were painful indications of the evolving new threat. Yet 9/11 was qualitatively different, in that it was the first large-scale attack

on the homeland, of a far larger magnitude than anything done before. Indeed, 9/11 was the equivalent of a declaration of war, of total war, on the USA. Moreover, it was a declaration of war by a diffused, amorphous enemy, who did not put forward a clear set of demands, or even a well defined set of grievances (that could be negotiated away, or mitigated). The nature of the threat, and the accompanying challenge to USA security are thus unprecedented.

The shock caused by 9/11 can be seen as a combination of Pearl Harbor and the Sputnik: a surprise attack resulting in initial stunning losses, the revelation of an unbearable degree of vulnerability, the birth of a major new threat to national security and the dearth of technological means to effectively face it. The latter is of course the key to the (re)design of a coherent defense R&D policy, having (once again) a well defined goal, namely, the development of the scientific and technological infrastructure to serve the long term war against terrorism. This goal has far reaching implications in terms of the direction of the defense R&D called forth, and, if pursued forcefully, would represent a significant departure from the kind of R&D done until then. Before analyzing in more detail what the war on terrorism requires, it is important to note what is ***not*** needed in this new era, thus suggesting a policy that involves primarily a ***reallocation*** of existing resources rather than increased expenditures.

II.1 Defense R&D Stocks

Following the collapse of the Soviet Union, there is no country (or plausible coalition of countries) that can challenge the present ***technological supremacy*** of the USA military.[7] Indeed, the defense R&D "stock" of the USA, developed and accumulated over the past decades, is far larger than that of any country(s) in the world.[8]

[7] I refer here just to the technological capabilities as manifested in the quality and effectiveness of the weapon systems, and not to the military stock, that is, the actual quantity of weapons (and manpower) available.

[8] R&D (or "Knowledge") stock is a widely used concept (see e.g. Griliches, 1984), paralleling that of physical capital stock, and can be computed simply by accumulating lagged R&D expenditures, and assuming a given depreciation rate, usually significantly higher than that for physical capital. It is not clear what rate would be appropriate for computing a defense R&D stock, presumably it varies *inter alia* with the intensity of the arms race. Here I shall use a depreciation rate of 15% (which has become a sort of "focal" figure in this type of computations), but compute the stocks also for a 5% rate, in order to gain an idea of the range of uncertainty in that respect.

The only other sizable stock was that of the USSR, but that has shrunk dramatically after the collapse, and Russia cannot afford to renew it.[9] Japan has severe built-in constraints on spending in defense R&D making it a non-contender for the foreseeable future. Western Europe has advanced technological capabilities but has spent an order of magnitude less than the USA for the past decades and, barring a dramatic geo-political change, it will continue to do so in the future.

In order to gain an idea of the actual magnitudes involved, I computed the defense R&D stocks generated during the decade of the 1990s (1991-2000) for the G8 countries that have had significant military R&D investments.[10] To insist, these are not the *total* stocks available, but only the portion added during the 1990s – these countries had substantial defense R&D stocks prior to that (particularly the US), generated during the long decades of the cold war. As table 1 reveals, the US accumulated during the 1990s an additional defense R&D stock over ***10 times*** as high as the next largest (the UK if using a depreciation rate of 15%), ***28 times*** that of Russia, and over ***3 times*** that of the other countries combined. These are stunning differences, which give a quantitative sense of the technological supremacy referred to above.

Some qualifications to these computations are in order. First, Table 1 quite likely overstates the actual technological gap between the USA and its allies, given that the USA exports to them military equipment embedding technological advances achieved by the R&D that goes into these stocks, and that some of the R&D projects are joint with them. On the other hand the extent of underreporting of defense R&D (due to secrecy – these are the so called "black programs") is likely to be significantly higher in the USA than in Western Europe. Second, there are likely to be spillovers and leakages from the defense R&D done in the USA that enhance the technological capabilities of other countries. It is hard to believe though that these qualifications would alter significantly the picture that emerges from Table 1.

[9] Note that Russia's GDP is at present just about *1/40* that of the USA.
[10] Thus we exclude Canada and Italy.

Table 1 **Defense R&D stock as of 2000** *(in billions of constant 1998 $ US)*[11]		
G8 Countries	*stocks based on a depreciation rate of:*	
	15%	***5%***
USA	**197.23**	**301.64**
United Kingdom	**18.21**	**28.03**
France	**17.81**	**28.69**
Japan	**9.96**	**14.78**
Germany	**9.18**	**13.47**
Russia	**7.14**	**11.06**

Beyond the advanced nations, China is perhaps the only emerging power that may be a source of concern. However, a simple calculation indicates that the possibility of China posing a serious challenge to the defense R&D advantage of the US is rather unlikely: the USA spends about 0.4 percentage points of GDP on defense R&D. Given that China's GDP is about one tenth that of the USA, in order to match the US current level of spending China would have to allocate a staggering 4% of its GDP to defense R&D, and maintain that level for many years, a rather farfetched scenario.[12] Furthermore, matching on a current basis would erase the initial huge advantage of the US only in the very long run. Essentially, the vastly larger economic resources of the USA *vis a vis* any other nation(s), and the fact that it already possesses a huge stock of military R&D gives the USA an unmatched technological advantage that cannot be challenged except if a

[11] The data used in these computations are in appendix 1. Note that there is a significant degree of uncertainty regarding some of these data, particularly that of Russia, and hence these figures should be taken as indicative only. To compute the stocks I simply apply the formula: $\sum_{t=0}^{9} D_{1991+t} \cdot (1-r)^{9-t}$, where D_{1991+t} denotes defense R&D expenditures in year 1991+t.

[12] One could argue that R&D costs in China are significantly lower than in the US, and hence matching the real amount of resources allocated by the US to defense R&D would entail significantly less than that. However, even if R&D costs were ***half*** as high in China, that still would entail allocating 2 % of GDP to military R&D, again a staggering amount. To put that figure in perspective, notice that the share of China's GDP devoted to ***total*** military expenditure was 1.4% in 2001 according to official Chinese figures, or 2.1% according to (SIPRI, 2002).

dramatic geo-political change occurs. However, even if that were the case the USA will still have significant margins of time (and resources) to respond.

II.2 The composition of defense R&D

How much does the US invest in R&D aimed at big weapon systems versus other technological means that could help confront current threats to national security? To address this issue I proceed to examine in detail the composition of the defense R&D budget for FYs 2001-2003. The Office of the Under Secretary of Defense (Comptroller) publishes a document named "RDT&E Programs", which contains a listing of almost 800 budget items, indicating the agency in charge, the type of program, the program name and the allocated budget (see appendix 2 for a listing of the top 20 items in the list). With the aid of expert officers of the Israeli Air Force, we managed to classify 369 out of the 798 items listed, which account for about 90% of the budget.[13] The categories used were:

- B – Big weapon systems
- D – Ballistic Missile Defense
- I – Intelligence
- T – Anti-Terrorism
- M – Miscellaneous (i.e. not elsewhere classified)

By "big weapon systems" I mean traditional, large, complex weapon systems having mostly an offensive character, such as jetfighters, ICBMs, carriers, nuclear submarines, and the like. We define a separate category for "ballistic missile defense", since these are *defensive* systems, relatively new, and meant to respond to present and future threats posed by the proliferation of long-range missile technologies to potentially hostile states. In case of doubt between "B" and "M" we opted for "M", in order to prevent biasing the totals in favor of the argument put forward here. Intelligence is almost certainly underrepresented in these data, if only because the funding of the Directorate of Science and Technology of the CIA is (as far as I know) not included in these figures. The "T" category is almost surely understated as well, since it is very hard to discern what exactly qualifies as "anti-terrorism": as it stands now it just includes all items

[13] We sorted the items by the allocated budget, and examined the items from the top down; thus, although we classified only ~ 50% of the items, they account as said for ~ 90% of the total budget.

related to chemical and biological warfare,[14] and a few others.[15] Moreover, the newly created Department of Homeland Security presumably commands additional budgets for antiterrorism-related R&D that are not included in our figures. "Miscellaneous" means "not elsewhere classified", that is, it is the default category for all items that do not clearly belong into one of the others. There are likely to remain significant margins of error in the classification performed and, in particular, intelligence and anti-terrorism are quite certainly downward biased; however, the summary results presented in Tables 2a and 2b are still hopefully informative and in the right ballpark:

Table 2a
Distribution of Defense R&D – 2001-2003
(current thousand $)

Category	**FY 2001**	**FY 2002**	**FY 2003**
Big weapons systems	10,752,781	11,911,890	13,805,069
Miscellaneous	12,107,023	14,029,675	14,407,247
Ballistic Missile Defense	4,302,183	7,039,441	6,848,958
Intelligence	2,953,072	3,378,629	4,490,930
Anti-terrorism	754,140	902,937	1,394,472
Not classified	4,497,512	4,081,025	4,178,031
Total[16]	***35,366,710***	***41,343,596***	***45,124,706***

Table 2b
Distribution of Defense R&D – 2001-2003
(percentages)

Category	**FY 2001**	**FY 2002**	**FY 2003**
Big weapons systems	30.40%	28.81%	30.59%
Miscellaneous	34.23%	33.93%	31.93%
Ballistic Missile Defense	12.16%	17.03%	15.18%
Intelligence	8.35%	8.17%	9.95%
Anti-terrorism	2.13%	2.18%	3.09%
Not classified	12.72%	9.87%	9.26%
Total	***100.0***	***100.0***	***100.0***

[14] Not all of it is related to anti-terrorism, but we could not tell that apart.
[15] There is only one item that explicitly mentions the war on terrorism, "Combating Terrorism Technology Support", Office of the Secretary of Defense, allocated just $49 million in 2003.
[16] The total amounts here are lower than the total defense R&D budgets (by about 10-15%): defense-related R&D done by other government agencies (such as NIH) is not included, there are other (apparently classified) items not reported in the published list, and moreover, some of the items listed in the cited document have not been assigned a dollar amount.

As Table 2 reveals, about 30% of the reported defense R&D is (still) allocated to big weapon systems. This category includes the development of systems that have no rival in the world, and moreover, it is not clear what sort of security threats these costly weapons are meant to forestall. The prime example is the F-22, a kind of technological marvel, extremely expensive aircraft, with projected capabilities beyond what could be regarded as real needs that current jetfighters could not appropriately fulfill.[17] On the other hand intelligence and anti-terrorism command only about 10-13% of the budget.[18] As argued in coming sections, even if the true figures are significantly higher than these the percentage allocated to these key activities is still quite low, relative to their present and future importance for national security. Therefore, it seems that the dramatic shift in the nature of the threats to national security since 9/11 have had so far little impact on the composition of R&D, and that calls for a prompt revision. One mitigating factor though may be just time: even if policy priorities shift, it takes a while to implement the desired changes, and in particular, it takes time to launch R&D programs to serve those changing priorities. For example, and as Figure 1 reveals, it took about 3 years to beef up NASA's budget after Sputnik – we are not there yet post 9/11.

III. The nature of the terrorist threat

Present day terrorism, as manifested most potently in 9/11, poses a very different set of threats than the conventional, nation-against-nation type of conflicts that have been prevalent throughout most of history.[19] Confronting such novel threats presents a formidable challenge at all levels: to the current military, intelligence and police capabilities of the target countries, to their democratic institutions that need to strike a

[17]As David Gold writes in SIPRI (2002), "The F-22…was designed during the cold war to counter an expected new generation of Soviet aircraft and air defenses that never materialized. The F-15, which the F-22 will replace, gives the USA air superiority over any conceivable enemy well into the future. Thus, the F-22 may be a system without a threat to combat…" Estimates are that a fully equipped plane will cost well above $100 million.

[18] Still, in (nominal) dollar terms intelligence and antiterrorist related R&D increased by over 50% from FY 2001 to FY 2003.

[19]It is also very different than previous instances of terrorism, particularly in that most terrorist organizations operated locally (within their own countries), and had as goals igniting some sort of drastic ***internal*** political change.

delicate balance in pursuing this war; and also to the scientific and technological resources that need to be mobilized in order to devise the appropriate technological means to combat terror. The later require the design of a coherent and well-articulated R&D policy, which should be based on the systematic analysis of the nature of these threats, in and of themselves, and in contrast to those posed by conventional conflicts. The goal of this section is thus to set the framework for such analysis, and in particular to try to identify the distinguishing features of the terrorist threat that have salient implications for R&D policy.[20]

Let me start with two general points. The first is that present day terrorism is based upon and exploits huge asymmetries between the perpetrators and the victims: asymmetry in the perceived value of life (leading *inter alia* to suicidal attacks); asymmetry in the means of combat (relatively simple for terrorists, highly sophisticated and powerful for the target countries); asymmetry in the information available on each side: mostly open information on the potential targets/victims, versus highly secretive, compartmentalized behavior of terrorists, and so forth. That is not so (for the most part) in conventional conflicts between nations, and therefore a great deal of the capabilities accumulated in any country in the course of contemplating or having been engaged in such conflicts are rendered ineffective for the war on terror. In particular, many of the weapon systems developed by the leading industrialized nations over the 20th century, and in particular those developed in the course of the cold war, are not appropriate to fight terrorism. Thus, R&D policy in this context will have to depart from established premises, and offer novel options.

The second observation is that one cannot expect a clear, decisive victory in the war on terror, that once and for all would defeat the enemy. Furthermore, in this kind of war there is no possibility of circumscribing the contest, the race, with formal agreements or treaties as those that were concluded with the USSR during the cold war. Therefore,

[20] In doing this we follow Arrow (1962), in the sense that the role of R&D and of government policy in this regard should follow from an understanding of the nature of the "good" in question: Arrow dissected the nature of knowledge and of knowledge creation, whereas here we are trying to understand the peculiarities

one should proceed on the premise that this will be a lengthy, protracted confrontation, entailing long-term, persistent threats. Accordingly, R&D aimed at it should be multi-layered in time, in the sense of being able to generate technological responses for the short, medium, and long run. I turn now to more specific characteristics of the terrorist threat: the key role of uncertainty, limited deterrence, and the private/public good aspects of providing security in this context.

III.1 The role of uncertainty

A key feature of the terrorist threat is the generalized, diffused nature of it, that is, the fact that there is a large degree of uncertainty regarding where, when and how terrorists may strike. Such uncertainty is what greatly magnifies the terrorist threat, far beyond what it would take to confront the terrorists if faced with them, or the actual damage that any single terrorist strike may cause. Indeed, if the authorities had advance knowledge of the timing and location of a future attack, actually thwarting it would be a relatively minor affair, involving the deployment of little police or military power.[21]

That is not so in conventional warfare: confronting say an invasion by a foreign power necessitates vast military capabilities, even if one knows when and where the attack will take place. The same applies to a nuclear confrontation: the "MAD" doctrine required that each party had the capability to nearly annihilated the other, regardless of being able to know in advance the timing and exact targets of an attack. In other words, the *sine qua none* to fight a conventional or even a nuclear war is a powerful army, measured by the strength and technological means available to its forces: surprise or not, in the end wars are decided by the outcome of the actual clash between the foe armies.[22] By contrast, fighting terrorism involves first and foremost reducing uncertainty, avoiding

---

of the war against terror, as opposed to conventional warfare, and derive from it the contours of an appropriate defense R&D policy.

[21] Consider for example what would have taken to prevent 9/11, had the FBI known in advance the plan: a score of arrests in several locations, conducted by a few hundred agents – a trivial operation relative to the magnitude of the threat.

[22] This is not the deny of course the role of surprise: when posed to launch the offensive on the Nazis, the allies invested great efforts in deception, that is, in creating uncertainty as to where and when D-day would take place. Yet, it is hard to imagine that any outcome of significance for the war depended upon the success of the deception campaign.

surprises. If we knew where say Al-Qaeda cells are, apprehending or destroying them would be a relatively easy task; likewise, if we could detect terrorists as they try to approach or enter a target, then neutralizing them should be the easy part. Even narrowing down the geographical area and/or the time window of a possible terrorist strike can greatly simplify the task of thwarting the attack.

The inherent uncertainty of the terrorist threat is also what exerts a heavy price on the threatened nation, far beyond the actual damage that may be inflicted once the attack occurs. That is, individual terrorist acts or even a series of them may not compromise national security at large, in the sense of hurting a large proportion of the civilian population, or damaging a significant chunk of the economy or, to take it to an extreme, posing a danger of losing sovereignty to a foreign power or to an alien extremist group. And yet the uncertainty as to when and where these acts may occur may have far reaching effects, both in terms of economic costs (e.g. the provision of security at a myriad potential targets, reduced investments because of generalized uncertainty, disruption of travel, tourism, and perhaps also trade), psychological costs, and painful changes in established norms, behaviors and "way of life" (e.g. invasion of privacy for the sake of prevention, avoidance of skyscrapers, reduced travel and tourism, etc.). It is precisely because of the uncertainty that accompanies the terrorist threat, and the associated costs, that few terrorists, armed with relatively primitive means, can effectively threaten whole countries, even the most powerful of them.

III.2 Limited deterrence

One of the novel and most disturbing aspects of present day terrorism is the fact that the perpetrators are ready to commit suicide in order to fulfill their mission, and furthermore, that some of their attacks are *based* upon suicide, as in 9/11. Indeed, there is a huge difference between readiness to die for a cause but still hoping to get away alive, and planning from the start to commit suicide in the course of the attack, as an integral and unavoidable part of the plan. Perhaps the most serious implication of the latter is that the possibility of deterrence is greatly reduced, at least in the sense that the perpetrators have nothing to fear for themselves. There still might be some deterrence possible if for

example the terrorists were based in a sympathetic host country (as was the case with Afghanistan), and hence the victim could retaliate against the host country; similarly if terrorists had families or wider social networks in known places that could be affected ex post. However, after the war in Afghanistan that seems to be less and less the case.

Limited deterrence implies that there is little use for offensive weapon systems that in conventional confrontations would be perceived by the potential attacker as posing an *ex post* threat. Thus, suicidal terrorism neutralizes to a large extent the initial advantage that advanced countries (the potential victims from terror) had in terms of military might, since such military capabilities are rendered vacuous by denying their deterrence value.

III.3 National Security: still a public good?

National defense (or national security) has been traditionally regarded as the prototypical type of public good.[23] This is not just a definitional matter, but has far reaching normative implications: given the "pure" public good nature of defense, economic logic has it that governments should be in charge of supplying it, and in fact have exclusivity at it. Moreover, doing so may be one of the main justifications for the very existence of a government, even in societies patterned after strict market principles. Indeed, defense ranks higher as a public good than, say, "maintaining Law and Order", since the latter could be provided by local communities in a decentralized fashion (as has been the case in many instances throughout history), whereas for a given political entity as a whole (e.g. "nation", "state") defense can hardly be decentralized. Let me restate those aspects of a good or service that make it "public" rather than private:[24] First, public goods are said to be *non-rival* in consumption, that is, the total amount of the good produced can be "consumed" by each and every individual in society. By contrast, the total amount of a private good produced is divided among consumers, so that if one consumes more others necessarily will consume less. Second, agents providing a private

[23] See for example Gold (1999) for a discussion of defense as a public good in the international context.

[24] In addition to these, the provision of some public and quasi-public goods entails indivisibilities, that is, minimal large-size investments in production, as for example with mass transport, dams, etc.

good can prevent others from getting access to the good and consuming it (for example, excluding those that refuse to pay for it), whereas there are no effective exclusion mechanisms for public goods. That is, it is hard or impossible to prevent anybody that so desires from getting access and enjoying the public good.

Thinking of national defense as protection from foreign threats that may in principle affect the country as a whole, it is clear that the two attributes of public goods strictly hold for it: (*i*) non-rivalry - each citizen enjoys the ***full*** amount of defense produced; (*ii*) it is impossible to exclude citizens that say, don't pay taxes, from enjoying the protection from foreign threats offered by the defense capabilities supplied in the country. However, and as the discussion below indicates, the nature of defense is much more complex in the context of the war against terrorism.

As already mentioned, a key feature of terrorism is that the threat is generalized (i.e. it can happen anywhere, anytime), and yet any particular attack is "local", in that it entails striking at a particular location that constitutes, even in the worse of cases, a small fraction of the country as a whole. Accordingly, confronting terrorism entails two very different strategies: the first consists of fighting the terrorist threat *at its source*, namely, intelligence gathering, pinpoint strikes at terrorist cells, denying bases in countries abroad, etc. The second entails deploying resources to protect likely targets in the homeland. It is intuitively clear that the first strategy does retain the public good nature of defense, whereas the second strategy makes the provision of defense mostly a *local* public good, even conveying *negative* externalities.

Consider for example the threat of terrorist bombings against civilian targets in the form of (local) public places that attract large numbers of people, such as shopping malls or big office buildings. In the absence of specific information on where and when the attack may take place, protecting against such threat involves setting up some form of security system at ***each*** such location. That may take the form of security guards, checks on each person entering the facility, metal detectors, sniffing machines for luggage, and so forth. Clearly, the deployment of a security system of that sort at a specific potential

target location serves first and foremost those present at or otherwise associated with that location, thus becoming a ***local*** public good. Moreover, increasing security at one particular location may actually increase the risk to adjacent locations, since terrorists are likely to prefer the least protected target – this is the negative externality mentioned above.[25]

In the case of airports the issue is more complex, as was painfully realized in 9/11: most of the victims were located far away from the departure sites and had nothing to do with air travel. In fact, securing airports serves a much wider purpose than just protecting those directly associated with it, and hence it is surely closer to a public good. In the case of public utilities, the effects of a terrorist attack may also be much wider in scope than those occurring at the plant itself and its immediate surroundings. As these examples reveal, there is actually a wide spectrum of possible cases, ranging from strictly local targets, to those that may serve just as entry points for more generalized threats, to targets that attacks upon them may have widespread repercussions. I focus in the analysis just on the polar cases in order to sharpen the issues at stake, but we should keep in mind that actual threats may lie somewhere in between.

These qualifications notwithstanding, terrorism has indeed caused national security to become partly a private good, and therefore the provision of defense is no longer strictly confined to the government, but has been to some extent "privatized." Of course, security in general (e.g. protection from local crime such as theft, violence, sabotage, industrial espionage) has always been to some extent privately supplied, and there is indeed a sizable cottage industry already in place that does that. In that sense the tension between the two strategies described above may be seen as a replay of the tension that may exist in any urban center between say preventive police action on the one hand, and placing private guards or security systems at specific locations on the other. There are of course huge differences between terrorism and traditional forms of crime, having to do primarily with the relative magnitude of the threats, the underlying causes and

[25] But there may be also positive externalities, as in other security context – see for example Ayres and Levitt (1998).

ultimate aims of each, and the national (and even cultural) significance of the threats. These differences surely enhance the role of the government in protecting from terrorism versus traditional crime, and yet there are wide margins left for the private provision of security. Moreover, distributional considerations for government intervention are surely more compelling in the case of terrorism.[26]

IV. A model of terrorism[27]

There are three parties involved in the "game" of terrorism: (*i*) the terrorists, whose aim is to inflict damage to potential targets, and hence their "utility" is a positive function of the losses suffered by their victims; (*ii*) the potential targets: think of them as firms that, absent terrorism would go about their business as usual and receive a certain payoff (e.g. profits, utility, rents), but under the threat of terrorism have to factor in the risk of being hit, loosing the payoff and incurring a further loss; (*iii*) the government, who maximizes the expected benefits accruing to the targets, taking into account the behavior of the other actors. The cornerstone of the model suggested here is the discrete choice problem facing the terrorists, which we think of as a nested model: the terrorists have to decide whether to strike or not, and if they do then which target to hit. This decision-making problem generates a set of probabilities over those possible actions. Potential targets can affect those probabilities through their decisions of how much to invest in their own security. Finally, the government decides how much to invest in fighting terrorism at its source, thus also affecting the probabilities attached to the various options facing terrorists.

---

[26] Distributional considerations refer to the fact that public places that cater to low-income segments of the population may invest little in security, and thus became more likely targets. However, such outcome may be perceived as unfair, much as denying medical care to those unable to pay for it is widely regarded as morally untenable.

[27] Enders and Sandler (1995) provide an excellent review of the economic literature on terrorism, both theoretical and empirical, up to early 1990s. Reflecting the nature of terrorism at the time, the dominant concerns addressed by this literature are (*i*) whether to bargain or not with terrorists posing concrete demands to governments; (*ii*) formation of treaties between countries to counter terrorism, and whether to abide or not by these treaties; (*iii*) strategic interactions between countries which are potential targets of terrorism. These issues lend themselves naturally to game theoretic analysis, which provides indeed with illuminating insights. The model developed here is similar in many ways to the formulations found in this literature (e.g. the decision tree of terrorists), but the focus is quite different. In particular, the interplay between government action and that of private potential targets, which is key here, seems to be altogether absent from previous models.

Let $j=1...n$ index potential targets. If hit, target j suffers a loss of L_j'; if not it carries on and receives a (normalized) payoff of 1. Each target spends x_j on its own security. Denoting $L_j = L_j'+1$, the (conditional) random utility of terrorists if hitting target j is,

$$(1) \qquad V_j = L_j - \beta x_j + \varepsilon_j$$

Thus, and conditional on striking, terrorists will chose a target so as to $\underset{j}{Max}\, V_j$. Assuming that ε_j is i.i.d. and has a Weibull distribution, the conditional probability that target j will be hit is the usual MNL,

$$(2) \qquad \pi_j = \frac{e^{L_j - \beta x_j}}{\sum_i e^{L_i - \beta x_i}}$$

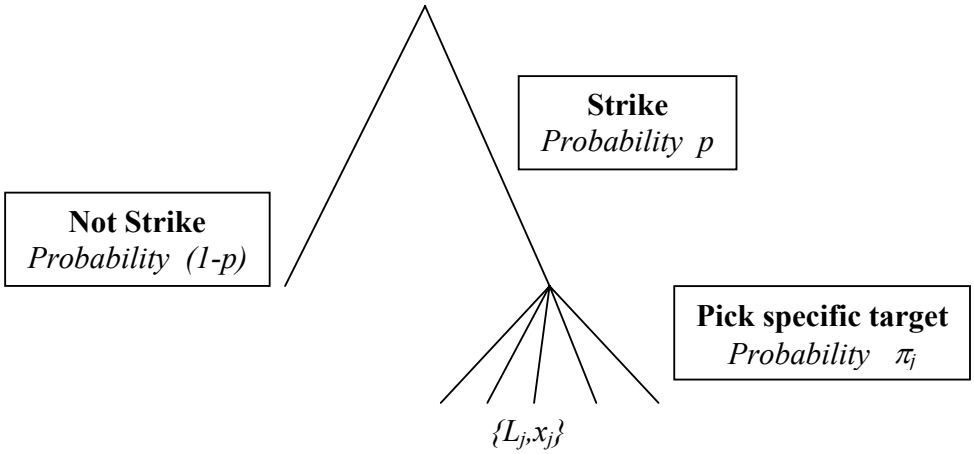
The "inclusive value" of the targets to the terrorists, i.e. the expected maximum utility if they strike is,

$$(3) \qquad I = \ln \sum_i e^{L_i - \beta x_i}$$

Denote by T the benefits to the terrorists of being able to carry a terrorist strike, beyond the damage it actually inflicts (i.e. the propaganda value, demonstration effect, chances of getting additional finance, etc.). Suppose that the government invests X in fighting terror at its source. Normalizing the value to the terrorists of ***not*** striking to 1, the probability that terrorists will strike is,

$$(4) \qquad p = \frac{e^{T - \alpha X + \lambda I}}{1 + e^{T - \alpha X + \lambda I}}$$

where $0 < \lambda < 1$ is the usual nested-logit parameter that mitigates the IIA problem,[28] and α stands for the "effectiveness" of the government's security outlays. Diagrammatically, the decision tree of terrorists is,



The *unconditional* probability of target j being hit is thus $p_j \equiv p\pi_j$. We can write now the objective function of target j, that is, the expected value of its net benefits,

$$(5) \qquad E_j = [1 - p_j(x_j)] - p_j(x_j)L_j' - x_j = 1 - p_j(x_j)L_j - x_j$$

Notice that not only π_j but also p are a function of x_j. However, if there is a large number of similar targets and hence the π_j's are very small (i.e. on the order of $1/n$), then the impact of a marginal change in the security outlays of any single target on p (i.e. on "overall deterrence") will be nil:

$$\frac{\partial p}{\partial x_j} = -\beta\lambda p(1-p)\pi_j$$

Therefore, we assume that when maximizing E_j target j takes p as given. Once again, being just one of many, it also takes as given the outlays of the other targets, hence,

[28] That is, if λ=1 we are back into the MNL for the whole choice set including the option of not striking, and therefore the ratio of the probability of not striking and of striking a particular target remains constant even if identical targets are added or removed, which is of course highly implausible.

$$\frac{\partial \pi_j}{\partial x_j} = -\beta \pi_j (1-\pi_j)$$

The FOC for *Max* E_j is simply,

$$(6) \quad \frac{\partial E_j}{\partial x_j} = \beta \pi_j (1-\pi_j) L_j p - 1 = 0 \quad \Rightarrow \quad \pi_j(x_j)[1-\pi_j(x_j)] = \frac{1}{\beta p L_j} \equiv c$$

Figure 2 presents a diagrammatic analysis of (6). Note first that, for any $0 \le \pi_j \le 1$, $\pi_j(1-\pi_j) \le 0.25$, and therefore for there to be a maximum the following condition needs to hold: $1/\beta p L_j \equiv c \le 0.25 \Rightarrow \quad p\beta L_j \ge 4$. That is, the losses, and/or the probability of a terrorist strike, and/or the effectiveness of the private security spending have to be "large enough" (for example, *c''* in Figure 2 does not fulfill this condition). Second, the conditional probability of a strike against target j should be at the optimum smaller than such probability if target *j* chooses not to spend any resources on its own security, that is, $\pi_j^* \le \underline{\pi}_j(0)$. Thus, in Figure 2 when the parameters are such that $1/\beta p L_j = c'$, the optimal level of spending is zero.[29] When these conditions hold, the provision of security from terrorist attacks turns in fact into a ***quasi private good***, that is, there are incentives for private parties to invest in their own security. As can be easily seen in Figure 2, x_j^* is an increasing function of $p\beta L_j$, i.e. each potential target will spend more on its own security the higher the probability that there will be a strike, the larger the expected losses, and the higher the "effectiveness" of its security outlays, β.

As already mentioned, target j sees the impact of x_j on p as negligible, and therefore disregards that effect when setting its optimal level of spending on security. But

[29] If $\underline{\pi}_j(0) < 0.5$ then the condition $\pi_j^* \le \underline{\pi}_j(0)$ is more stringent than the former, in that it requires that $p\beta L_j$ be even larger for there to have $x_j^* \ge 0$.

what about spending ***voluntarily*** on *X*, that is, on fighting terror at its source, thereby bringing p down directly? Writing $E_j = 1 - \pi_j p(X) L_j - X$, we note that the FOC for $\underset{X}{Max} E_j$ is,

$$(7) \qquad p(X)[1 - p(X)] = \frac{1}{\alpha \pi_j L_j}$$

Comparing (7) to (6), and assuming for the moment $\alpha \approx \beta$, we see that in the denominator of the r.h.s. of (7) we have π_j rather than p in (6), and that makes the whole difference: once again, the basic assumption is that there are very many targets, π_j is very small (on the order of 1/n), and in particular $\pi_j << p$. Therefore, whereas the condition for there to be an optimal $x_j > 0$ is likely to hold, that is not so for there to be an optimal (private) $X>0$. Thus, it is highly unlikely that private parties would be willing to contribute voluntarily to fighting terror at its source, and hence that role is left to the government. On the other hand it is plausible that each potential target will spend on its own security.

The provision of security against terror takes then a dual nature: a ***public good*** on the one hand (i.e. reducing the likelihood of a strike by fighting terror at its source), which is the traditional case, and a ***quasi private good***, namely, each potential target spending on its own security.

IV.1 Externalities

As opposed to the classic case of defense as a pure public good, in the present case a dollar spent on enhancing the security of a potential target has two opposite effects. The first is zero-sum: conditional on a strike taking place, an extra dollar of x_j decreases the probability of a strike against target j, and thereby it necessarily ***increases*** the probability of the other potential targets being hit. That is, enhancing the security of a particular target confers a ***negative*** externality to all other potential targets. On the other hand, an increase in x_j reduces the inclusive value of striking (i.e. it lowers *I* in (4)), which lowers p and hence confers a ***positive*** externality. That is, enhanced security at

any particular target reduces the attractiveness of striking in general, and hence lowers the likelihood of an attack for everybody.

The net effect though is negative: Denoting by $p_{i\neq j} = p(1-\pi_j)$ the unconditional probability of targets other than j being hit, we show in appendix 3 that $\partial p_{i\neq j} / \partial x_j > 0$. That is, the net impact of enhancing the security of a particular target is to increase the risk faced by others.

IV.2 The relative effect of X versus x_j

From the point of view of society as a whole, the key issue is how to reduce p, the likelihood of a strike. Thus, one way of assessing the relative effectiveness of the two types of expenditures on security, X and x_j, is to compare their effect on p. Recall that,

$$(8) \qquad \frac{\partial p}{\partial X} = -\alpha p(1-p) \text{ , and } \frac{\partial p}{\partial x_j} = -\beta\lambda p(1-p)\pi_j$$

Thus, and assuming for a moment that $\pi_j \approx 1/n$ and $\alpha \approx \beta$, a marginal dollar spent on X is about ***n/λ*** **times** as effective as a dollar spent on x_j. In other words, the per dollar benefits of devoting resources to fight terror at its source, which constitutes a public good, are much larger than those derived from enhancing the security of individual targets. This is hardly surprising, but the magnitude of the difference is sobering.

IV.3 How much X versus x?

The analysis so far provides the background for one of the key questions that arise in this context, namely, how much should the government invest in the ***S***-strategy, taking into account of course the behavior of the other parties to the game. We can think of the government as maximizing the expected value of the benefits to potential targets, net of the costs of investing in the ***S*** and ***L***-strategies. In the symmetric case (i.e. when $L_j = L$ for all j), the objective function is (recall that the payoff to each target is assumed to be 1),

(9) $W = p\ (n - L) + (1 - p)\ n - nx - X = n - pL - nx - X$

That is, with probability p there will be an attack on a particular target, which will incur a loss of $L = (L'+1)$, and thus total benefits will be just $(n - L)$, whereas with probability $(1 - p)$ there is no attack and hence benefits are n. Each target spends x on its own security, and the government spends X on the ***S***-strategy. The government moves first and sets X, taking into account how targets will behave in the second stage, when setting x optimally. Hence,

(9)' $W = n - p[x(X), X]\ L - nx(X) - X$

Maximizing (9)' the FOC is,

(10) $$\frac{\partial W}{\partial X} = -L\left[\frac{\partial p}{\partial x}\frac{\partial x}{\partial X} + \frac{\partial p}{\partial X}\right] - n\frac{\partial x}{\partial X} - 1 = 0$$

In the symmetric case, with $\pi_j(x_j) = 1/n$, the optimality condition for each target becomes,

(11) $$(1/n)(1 - 1/n) = \frac{1}{\beta L p[x(X), X]}$$

Notice that L, n, and β are parameters, and hence what adjusts is $p[x(X), X]$: given X, targets will invest in x so as to make the condition hold. Thus, in equilibrium,

(12) $$\frac{\partial p}{\partial x}\frac{\partial x}{\partial X} + \frac{\partial p}{\partial X} = 0$$

Therefore (10) becomes simply,

(13) $$-n\frac{\partial x}{\partial X} = 1$$

Note from (12) that $\frac{\partial x}{\partial X} = -\frac{\partial p/\partial X}{\partial p/\partial x}$. In the symmetric case *all* targets move in unison, hence, $\frac{\partial p}{\partial x} = -\beta\lambda p(1-p)$. Thus, using (8), $\frac{\partial x}{\partial X} = -\frac{\alpha}{\beta\lambda}$, and (13) becomes,

$$(13)' \qquad -n\frac{\partial x}{\partial X} = n\frac{\alpha}{\beta\lambda} \stackrel{?}{=} 1$$

Given that the l.h.s. of (13)' is made up of parameters, this equality obviously cannot hold but by coincidence. Notice that $\lambda<1$, and that n is supposed to be very large, hence normally $n\frac{\alpha}{\beta\lambda} >> 1$.

The meaning of (13)' is quite transparent: starting from any given $X>0$, either there is an equilibrium $x>0$ given by (11), or $x=0$. If the former is true, then a small change in X would lead targets to readjust as shown, e.g. an increase in X by one dollar decreases each target's spending on own security by $\alpha/\beta\lambda$. Since all targets behave the same way, the total savings of resources in local security are $n\alpha/\beta\lambda$. On the other hand the extra cost of spending an additional dollar on the ***S***-strategy is just that, one dollar. Thus, (13)' just says that the government should increase its spending until the marginal gain (in terms of savings in local security), $-n(\partial x/\partial X)$, equals the marginal cost. But savings are bounded from below by the fact that $x\geq 0$, and since both marginal gains and costs are constant, the equality cannot hold. The optimal amount of spending on the ***S***-strategy, to be denoted by X^* is thus given by,[30]

$$(14) \qquad (1/n)(1-1/n) = \frac{1}{\beta L p[0, X^*]}, \quad (\text{where } x(X^*) = 0)$$

[30] Conditions for the existence of X^* are given in Appendix 3.

The model thus provides a clear, sharp-edged answer to the question posed: ***the government should spend on fighting terrorism at its source as much as it takes so as to induce private targets to spend <u>nothing</u> on local security***. In other words, the optimal rule is that the government should bring p down (via expenditures in the ***S***-strategy) to the point where individual targets find it not worth it investing in their own (local) security.[31]

Ideally then we should see large amounts of resources being spent on intelligence and related ***S***-strategy activities, and ***none*** on the ***L***-strategy. In practice though we see large and increasing amounts being spent on local security. That may be so for two reasons: (*i*) the government does not spend enough on the ***S***-strategy; (*ii*) individual targets overestimate the probabilities that they will be hit, or otherwise attach additional psychological benefits to local security that go beyond the stark logic of our models. Further research is needed to elucidate these issues.

Some qualifications of this key result are in order. First, the costs of financing the ***S***-strategy are assumed to be linear, that is, each additional dollar "costs" the same regardless of how much the government spends. However, if it gets increasingly costly to finance spending on the ***S***-strategy (for example, if the government has to resort to more distortionary taxes, or to borrow at increasingly higher interest rates), then one may obtain a solution by which the optimal spending on the ***S***-strategy stops short of nullifying the incentives of potential targets to spend on the ***L***-strategy. However, this is a rather unlikely scenario, in view of the fact that spending on ***S***-strategy-related activities constitutes a very small fraction of the federal budget. In addition, it is not clear why the costs of government finance would be more convex than those of the private sector (potential targets), which is what is needed to alter the result. Similarly, one could consider breaking the linearity in the benefits side, for example by postulating β not as a constant but as a decreasing function of X, possibly leading to an interior solution with

[31] Note that in the classic case of a public good (such as national defense), the government has to supply it because there are ***no*** private incentives to do so (at least not in the required quantities); by contrast, in the present case the government has to allocate enough resources to the public good so as to ***prevent*** private agents from spending on (local) security, because such spending is highly inefficient.

$x^* > 0$. These are legitimate variations to be considered, and hence the basic result $x(X^*)=0$ should be regarded as a benchmark, to be revised as we learn more about the determining factors.

IV.3 The impact of R&D

R&D can be thought of in the present context as innovative activity aimed at increasing the effectiveness of spending on security, which in terms of the model means increasing the parameters α and β. Taking again reductions in p as the criterion for effectiveness, the impact of a marginal dollar spent on R&D is,

$$\frac{\partial p}{\partial \alpha}\alpha' = -p(1-p)\alpha' X$$

$$\frac{\partial p}{\partial \beta}\beta' = -p(1-p)\beta' \sum_i \pi_j x_j$$

where $\alpha' = \partial\alpha / \partial R\,\&\,D$, and similarly for β'. Thus, assuming for the moment that $\alpha' \approx \beta'$, R&D devoted to fighting terrorism at its source is likely to be much more effective than R&D aimed at local security, since surely $X >> \bar{x} = \sum_i \pi_i x_i$, that is, since the ***total*** expenditures on fighting terrorism at the source are surely larger than the ***average*** expenditure on own security by individual targets. In addition, $\lambda < 1$, which further plays in favor of α .

V. R&D to counter terrorism – policy implications

The dual nature of defense in the context of the war against terrorism maps also into the allocation of resources to R&D: should the Government engage in and/or pay for R&D aimed at improving the means available to both fight terror at its source and protect the population from its consequences? First, we know that even in the context of purely private goods, a market economy may well underinvest in R&D: the fact that R&D generates spillovers implies that the social rate of return is typically higher than the

private return, and hence that private investment in R&D may fall short of the socially desirable level. Thus, even if providing security from terrorism was deem to be entirely a private good, there would be room for government support to antiterrorism-related R&D, for example in the context of the Advanced Technology Program (ATP).

As we have seen though, there is a component of the fight against terror that clearly has a public good nature, and that is the one associated with the ***S***-strategy, that is, security outlays aimed at diminishing ***p***, the likelihood of a terrorist strike. This involves locating, monitoring and intercepting terrorist cells around the world, disrupting their logistical and financial base, limiting their access and mobility, and so forth, so that the ability or readiness of terrorists to carry out attacks are impaired as much as possible. Therefore, R&D aimed at enhancing the effectiveness of these outlays should be the government's responsibility, much as the provision of traditional national security-related R&D has always been.[32] One of the key aspects of the ***S***-strategy is intelligence, that is, the gathering of information on terrorists – masterminds, operatives, and supporters – their modes of operation, sources and channels of finance, and above all, as much detail as possible on their future plans. As noted in section III, one of the distinguishing features of the terrorist threat is the generalized, diffused nature of it, that is, the fact that there is a great deal of inherent uncertainty regarding where and when terrorists will strike. Intelligence broadly means the reduction of such uncertainty, it conveys vast, generalized benefits, and therefore it is the crucial tool and the preeminent public good in the context of the fight against terror. R&D aimed at providing better intelligence capabilities has therefore very high social payoffs, suggesting that it should be made the cornerstone of R&D policy in the war against terrorism.

In terms of R&D aimed at the ***L***-strategy, there may be a role for the government even though it is quite likely that local security would be provided privately, since as

[32] Notice that, as with traditional national security, that does not necessarily mean that the R&D should be performed by government agencies, nor that the government should necessarily pay for all or most the R&D costs: as long as the Government commits to purchase the security products that result from the R&D, private suppliers may share the R&D costs and the associated risks.

already mentioned, the market may still underinvest in R&D for the usual reasons.[33] Furthermore, there is certainly a role for the government in promoting ***basic research*** that feeds into down-the-line R&D aimed at enhancing local security, much as it does for most basic research in virtually all areas of science and technology: ever since Arrow (1962), it is well understood that basic research generates the most spillovers, the benefits from it are inherently very hard to appropriate, and hence it is up to the government to promote and subsidize it.

There are two additional areas that also call for a government role: R&D aimed at protecting from non-conventional terrorists threats (see appendix 4), and R&D for improved cyber security. The former differs from a conventional terrorist threat obviously in the scope of the potential damage, making them a "macro" threat and thus turning the provision of security against them into a classic public good, with the usual implications. With the proliferation of internet-based or just interconnected computerized infrastructure systems, threats at computer and communications networks have acquired once again a "macro" dimension (again, because of the scope and reach of the damage that may be inflicted), and therefore it is upon the government to play a key role in confronting them, particularly in the conduct of R&D.

Beyond R&D in purely technological fields, research in the behavioral and social sciences may also play a significant role in confronting terrorism: first, in understanding the motivations, the psychological makeup and the wider sociological context of terrorists, as well as contributing cultural, political and economic factors. Second, in dealing with the psychological and socio-economic effects of the terrorist threat on the targeted population, including the perception of probabilities that influences in turn the incentives to invest in local security.

[33] This is so in spite of the fact that, as mentioned in section IV, the level of spending in local security should be zero, provided that the government spends "enough" on the ***S***-strategy.

V. Defense R&D: technological directions and market competition

Both intelligence and protection of potential targets require the development of sensory computer interfaces, to be used for detection and intelligence gathering. As the analysis above suggests, increasing detection capabilities (in the broad sense), should be one of the main goals of defense R&D. The protection of targets as well as the identification of suspects require enhanced ability to detect weapons, explosives, bacteriological materials and other potentially dangerous devices, being carried by individuals, shipped over different means of transportation, stored in hidden places, etc. It also requires positive identification of individuals, both of suspects and of those with legitimate access permits to designated places.

These screening and detection capabilities should allow for the fast and reliable screening of people, containers, and luggage with minimal disruption to economic activity, travel, and privacy. This is a very tall order, considering the staggering number of people going daily through airports and other transport modes, entering big office buildings, government offices, infrastructure facilities, and similarly for the number of containers shipped, parcels mailed, and so forth. Another set of capabilities that need to be enhanced are those related to eavesdropping and interception of all sorts of communications, ranging from those taking place over regular phone lines anywhere in the world, to conversations inside caves in eastern Afghanistan, or in underground parking lots in New York.

The common denominator of this vast array of required capabilities is that one needs to be able to *emulate* human senses (to hear, to "see" and "recognize", to smell, to "touch and feel") in automated, computerized ways. That is, one needs to create smart, sensory interfaces between computerized detection systems and the physical world, that will be able to activate those senses in fast, reliable ways as a matter of routine.[34]

[34]See for example Appendix 3: "A collaborative effort…will investigate the reliable identification of specific individuals, even when attempts have been made to alter appearance, by measuring the "biometric" signatures of people passing through, for example, airports. The effort will range from development of surveillance sensors to algorithms that interpret their data and automatically alert operators to potentially dangerous people."

I emphasize this required change in the direction of technical change (i.e. emulating human sensory perceptions), because in fact computer technology has developed historically in a very asymmetric, skewed way vis a vis human capabilities: it sought relentlessly to improve the "brain" (i.e. the central processor), while keeping a primitive sensory interface. Call it the "Helen Keller model" of computer technology: virtually deaf, dumb, blind, (and lacking also tact or smell), but highly intelligent (i.e. capable of performing enormous amounts of routine computations). This has been, on reflection, a very peculiar path of technological development, dictated in part by the constraints of scientific knowledge, but also by the predominant type of uses that computers were put to work on.

There is however increased recognition that developing computerized sensory interfaces is extremely important for a wide and rapidly expanding array of civilian uses, ranging from automobiles (e.g. voice-activated computerized commands, improved safety technologies, preventive maintenance, etc.), to medicine, to consumer appliances and gadgetry. This is in fact one of the technological frontiers attracting a great deal of attention, both in basic and applied research. Thus, defense R&D devoted to this area is very likely to have ***immediate, direct*** spillovers to civilian uses. Presumably, there have been spillovers from "traditional" defense R&D all along (even if these are hard to quantify). The difference is that in this case the technological frontier that defense (anti-terror) R&D is supposed to push is the same as that required for progress in civilian uses. That is not the case with, say, improvements in nuclear weapons or in stealth technology: in those cases the gradient of technological advance in military R&D has no direct relevance for civilian purposes, and the spillovers, if at all, are only indirect.

Another area that calls for increased R&D resources is fast analysis of vast amounts of information, as best exemplified by the need to go over staggering amounts of voice, data and email messages intercepted by the NSA and other agencies (referred to as "fusion"). It would seem that the rate of growth of communications (i.e. of the amount of messages being transmitted over an expanding range of modes: fixed line and cellular

phones, satellites, the various wireless modes, fax, email) is at least as fast if not faster than the rate of improvement in computer capabilities aimed at analyzing them. Thus, in order to shorten substantially the delays in doing so (that have proven critical for the ability to identify terrorist threats in "real time"), the technologies in question would have to undergo significant breakthroughs. Again, this gradient of technological progress fits also well-defined civilian needs, as for example in terms of the data analysis requirements associated with the genome project and its aftermath (and even more so the corresponding program for mapping proteins), or more generally "data mining" in businesses, that has become an increasingly important activity in a wide range of sectors.

What is required then is the setting up of R&D programs that would support mainly the development of sensory computer interfaces for detection and intelligence gathering, and of computer technologies for massive data analysis. As said, the systems sought are for the most part "dual use", in the sense that they have both defense and civilian applications to begin with.[35] This is very different from cold-war defense R&D, aimed primarily at big weapon systems. As to the overall budget for defense R&D, the point emphasized here is the internal reallocation required, away from big weapon systems, and towards the new programs; it remains to be seen how the total would be affected.

The different nature of the new defense R&D may have profound implications for the industrial organization aspects of the sectors involved. The development of big weapon systems in the decades of the cold war lead to high concentration of both R&D and procurement into a few large corporations, conferring them a great deal of market and bargaining power. It is quite likely that this had detrimental effects in terms of costs and efficiency, and it may have steered technical advance into questionable directions (such as with the extremely expensive stealth technology). By contrast, the development of sensory computer interfaces, computer technologies for massive data analysis, Internet security, biological protection means, and the like, entails an entirely different playfield. These systems are by and large dual use, there is (also) a private market for many of the

[35] See Cowan and Foray (1995), Lerner (1992), and Molas-Gallart (1997).

products sought, and there exist already a vast number of players in the high tech, computer and biotech sectors that can partake in this new R&D, as well as attracting new entrants. R&D programs designed so as to preserve this diversity and to encourage further competition may prove highly beneficial both for the required defense R&D and for the advanced sectors of the economy themselves, thus fostering economic growth.

VII. Concluding remarks

The foregoing analysis of the threats facing the USA in the wake of 9/11 suggests the articulation of a coherent defense R&D policy based on the following set of principles:

- In view of the nature of the threats facing the USA, it is no longer clear whether it is still justified to devote large amounts of R&D to the development of costly big weapon systems, such as new jet fighters, nuclear subs, carriers, etc. Gradual upgrades of existing systems, and basic research for future generations may suffice. The resources thus saved could be reallocated to the development of intelligence enhancing and anti-terrorist means.

- The war against terrorism involves two main aspects: fighting terrorists at their source (the ***S***-strategy), and protecting potential targets (the ***L***-strategy). The former is a preeminent public good and hence should be supplied by the government, whereas the latter is typically a private or a local public good that carries negative externalities, and is far less efficient that fighting terrorism at the source. A key result of the formal analysis is that the government should devote enough resources to the ***S***-strategy so as to dissuade potential targets from spending on their own security. The different nature of each strategy dictates also the kind of R&D called for.

- Resources devoted to the ***S***-strategy involve monitoring and intercepting terrorist cells around the world, disrupting their logistical and financial base, limiting their access and mobility so as to impair their ability to carry out attacks, etc. This involves first and foremost ***intelligence*** activities in their broadest sense,

suggesting that the most important goal of defense R&D should be to provide advanced technological means in order to enhance the intelligence capabilities of the various agencies in charge, and of the supporting military forces.

- Protecting potential targets is a mixed public-private good, and typically we can expect indeed that individual targets will have incentives to invest in their own (local) security. If so, private firms will also have incentives to conduct R&D aimed at developing (more effective) means of providing local security. However, that may not be enough for the usual reasons, and moreover, the conduct of the required ***basic*** R&D necessitates government support, as is the case in virtually all realms of science and technology.

- R&D aimed at protecting from non-conventional terrorists threats, and R&D for cyber security call also for an active government's role, since both constitute "macro" threats and therefore the provision of security against them can be seen as a classic public good, with the usual implications. There is also room to encourage research in the behavioral and social sciences, aimed at understanding both the enemy and the effects of the terrorist threat on the targeted population.

- The provision of advanced means for intelligence and for target protection entails emulating human sensory perceptions through computerized sensory interfaces, and increasing the ability to analyze vast amounts of information. Both have direct civilian applications, and therefore the required R&D is mostly "dual use". Indeed, and contrary to the high concentration of defense contractors during the cold war era, the development of sensory computer interfaces, data mining, and the like, entails an entirely different playfield: there is (also) a private market for these dual use systems, and there exist already a large number of players that can partake in the required R&D. New R&D programs designed to preserve this diversity and to encourage further competition, may prove beneficial both for the required defense R&D and for the economy at large.

References

Arrow, Kenneth J., "Economic Welfare and the Allocation of Resources for Inventions," in R. Nelson (ed.), The Rate and Direction of Inventive Activity. Princeton University Press, 1962.

Ayres, Ian and Steven Levitt, "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack." Quarterly Journal of Economics, February 1998; 113(1), pp. 43-77.

Cowan, Robin and Dominique Foray, "Quandaries in the Economics of Dual Technologies and Spillovers from Military to Civilian Research and Development." Research Policy, 24, 1995, pp. 851-868.

Enders, Walter and Todd Sandler, "Terrorism: Theory and Applications". In Hartley, K. and T. Sandler (eds.), Handbook of Defense Economics, Vol. 1. Elsevier Science B.V., 1995.

Gold, David, "Does Military R&D Generate International Public Goods?" United Nations Department of Economic and Social Affairs, mimeo, January 1999.

Griliches, Zvi, ed. R&D, Patents and Productivity. University of Chicago Press, 1984.

Hoge, James F. and Gideon Rose (eds.), The War on Terror. New York, Council on Foreign Relations Press, 2002.

Lerner, Joshua, "The Mobility of Corporate Scientists and Engineers between Civil and Defense Activities: Implications for Economic Competitiveness in the Post-Cold War Era." Defense Economics, August 1992; 3(3), pp. 229-42.

Lichtenberg, Frank, "Economics of Defense R&D," in Hartley, K. and T. Sandler (eds.), Handbook of Defense Economics, Vol. 1, Amsterdam, Elsevier, 1995.

Molas-Gallart, Jordi, "Which way to go? Defense technology and the diversity of "dual-use" technology transfer." Research Policy, 26, October 1997, pp. 367-385.

Mowery, David and Nathan Rosenberg, Technology and the Pursuit of Economic Growth. Cambridge University Press, 1989.

SIPRI (2002), SIPRI Yearbook 2002: Armaments, disarmament and international security, Oxford: Oxford University Press, pp. 251, 309-322

US Government, Office of the Under Secretary of Defense (Comptroller), Department of Defense Budget, Fiscal Year 2003. Washington D.C., February 2002 (http://www.dod.gov/comptroller/fy2003budget/).

US Government, Executive Office of the President of the US, Office of Science and Technology Policy. FY 2003 R&D Budget Documents. Analytical Perspectives: R&D Chapter, Budget of the United States Government, Fiscal Year 2003 (http://www.ostp.gov/html/ap08.pdf)

US Government, Executive Office of the President of the US, Office of Science and Technology Policy. FY 2003 R&D Budget Documents. Antiterrorism S&T (http://www.ostp.gov/html/AntiTerrorismS&T.pdf)

Appendix 1
Defense R&D Expenditures – 1991-2000
(billions of constant 1998 dollars)

	USA		Germany		France		United Kingdom	
	$	**% GDP**	**$**	**% GDP**	**$**	**% GDP**	**$**	**% GDP**
1991	41.04	0.59	1.77	0.140	6.13	0.47	4.47	0.38
1992	43.74	0.59	2.18	0.108	4.99	0.38	4.67	0.39
1993	36.59	0.49	0.73	0.036	3.22	0.24	3.74	0.30
1994	38.64	0.5	1.87	0.089	3.74	0.28	2.70	0.21
1995	37.61	0.48	1.25	0.06	4.36	0.32	3.22	0.25
1996	34.59	0.43	0.93	0.044	3.95	0.29	3.64	0.27
1997	38.75	0.46	2.18	0.106	2.70	0.19	3.43	0.25
1998	35.80	0.40	2.18	0.099	2.18	0.15	3.01	0.21
1999	35.43	0.39	1.79	0.079	2.91	0.19	3.26	0.22
2000	34.97	0.38	1.76	0.079	2.88	0.19	3.30	0.22

	Japan		Russia	
	$	**% GDP**	**$**	**% GDP**
1991	1.56	0.05	1.96	0.34
1992	1.80	0.045	1.87	0.36
1993	1.82	0.045	1.66	0.36
1994	1.83	0.05	1.19	0.29
1995	1.85	0.045	1.27	0.35
1996	1.88	0.045	0.92	0.29
1997	1.89	0.045	1.35	0.30
1998	1.89	0.05	1.16	0.42
1999	1.89	0.05	1.26	0.32
2000	1.90	0.05	1.41	-

Sources:
G7 countries: Defense R&D computed from data taken from the National Science Foundation, Division of Science Resources Statistics (NFS/SRS), Appendix Table 5-41, and from SIPRI Yearbook 2002 (for total military expenditure). ***Japan***: defense R&D expenditures estimated as comprising 5% of total military expenditure. For 1999-2000, all countries other than the USA: extrapolation based on mean (defense R&D/total military expenditures) ratio for 1996-98. ***Russia***: total military expenditures: SIPRI (2002); defense R&D as % of defense budget: Ministry of National Defense, Republic of Korea (website: www.mnd.go.kr); GDP: World Bank and IFS. For 1992-93: extrapolation on the basis of the mean (defense R&D/total military expenditures) ratio for 1994-96. For 1991: extrapolation based on mean (defense R&D/GDP) ratio for 1992-94.

Appendix 2

Sample list (20 top items) from the Defense Department RDT&E Programs[36]

Source: http://www.dod.gov/comptroller/fy2003budget/

Org Name	PE Name	Category	2003 budget
Ballistic Missile Defense Organization	Ballistic Missile Defense Midcourse Defense Segment	D	3,195,104
Air Force Budgtd by DoD	Joint Strike Fighter EMD	B	1,743,668
Navy Budgeted by DoD	Joint Strike Fighter (JSF) - EMD	B	1,727,500
Ballistic Missile Defense Organization	Ballistic Missile Defense System Segment	D	1,065,982
Ballistic Missile Defense Organization	Theater High-Altitude Area Defense System – TMD - EMD	D	932,171
Army Budgeted by DoD	Comanche	B	914,932
Air Force Budgtd by DoD	Advanced EHF MILSATCOM (SPACE)	BI	825,783
Air Force Budgtd by DoD	Space Based Infrared System (SBIRS) High EMD	I	814,927
Ballistic Missile Defense Organization	Ballistic Missile Defense Boost Defense Segment	D	796,927
Navy Budgeted by DoD	SC-21 Total Ship System Engineering	B	717,397
Air Force Budgtd by DoD	F-22 EMD	B	627,266
Defense Adv Research Projects Agcy	Materials and Electronics Technology	M	440,500
Defense Adv Research Projects Agcy	Computing Systems and Communications Technology	MI	424,940
Navy Budgeted by DoD	V-22A	B	420,109
Air Force Budgtd by DoD	Test and Evaluation Support	M	398,266
National Security Agency	Information Systems Security Program	I	394,257
Navy Budgeted by DoD	Defense Research Sciences	M	393,557
Ballistic Missile Defense Organization	Ballistic Missile Defense Sensors	D	373,447
Air Force Budgtd by DoD	NAVSTAR Global Positioning System (Space and Control Segments)	BI	324,098

Categories:

- B – Big weapon systems,
- I – Intelligence
- T – Anti-Terrorism
- M – Miscellaneous
- D – Ballistic Missile Defense

Two letters (such as "BI") mean that the item is deemed related to both categories; in the calculation of expenditure shares per category, the expenditure is then split in half.

[36] Ranked according to the 2003 budget allocations.

Appendix 3

3.1 Proof of negative externalities

$$\frac{\partial p_{i\neq j}}{\partial x_j} = \frac{\partial p}{\partial x_j}(1-\pi_j) - \frac{\partial \pi_j}{\partial x_j} p$$

$$\frac{\partial p}{\partial x_j} = -\beta\lambda p(1-p)\pi_j, \quad \frac{\partial \pi_j}{\partial x_j} = -\beta\pi_j(1-\pi_j)$$

$$\frac{\partial p_{i\neq j}}{\partial x_j} = -\beta\lambda p(1-p)\pi_j(1-\pi_j) + \beta\pi_j(1-\pi_j)p =$$

$$= \beta p\pi_j(1-\pi_j)[1-\lambda(1-p)] > 0$$

since $1-\lambda(1-p) = 1-\lambda+\lambda p > 0$ (recall that $0 \le \lambda \le 1$)

3.2 Second order conditions for Max E_j:

$$\frac{\partial^2 E_j}{\partial x_j^2} = \beta L_j p\left[\frac{\partial \pi_j}{\partial x_j}(1-2\pi_j)\right] \Rightarrow \frac{\partial^2 E_j}{\partial x_j^2} < 0 \text{ } \textit{iff} \text{ } \pi_j < 0.5, \text{ since } \frac{\partial \pi_j}{\partial x_j} < 0$$

3.3 Existence of X^*

We have seen in ***IV.3*** that the optimal government spending on the S-strategy is given by,

$$(14) \qquad (1/n)(1-1/n) = \frac{1}{\beta L p[0, X^*]}, \quad (\text{where } x(X^*) = 0)$$

Such a X^* exists provided that for any $X<X^*$, $x(X)>0$, which in turn implies that,

$$\textbf{(A.1)} \qquad p(0,0) > \frac{1}{\beta L(1/n)(1-1/n)}$$

That is, if the government spends nothing on X the probability of a strike is high enough to induce targets to spend on their own security, thus lowering p up to the point where equality is restored as in (14). If (A.1) does not hold then $x=0$ regardless, and hence (9)' becomes simply $W = n - p(X)\,L - X$, leading to the FOC $\alpha Lp(1-p)=1$, i.e. the government will choose X^* such that $\alpha Lp(X^*)[1-p(X^*)]=1$. However, this case in rather uninteresting, in that we do observe private spending on local security even with $X>0$, and hence we can safely assume that (A.1) holds.

Appendix 4
OSTP, FY 2003 R&D Budget Documents - ANTITERRORISM S&T

The President is committed to leveraging the capabilities of our nation's scientific and engineering communities in countering new threats to our homeland and our national security. The President's 2003 Budget represents an escalation in the Administration's strong support for research and development aimed at defeating these dangers to our way of life. Research and development funding for homeland security and combating terrorism (including protecting critical infrastructure) will rise from nearly $1 billion in 2002 to an estimated $3 billion in 2003**.** These funds will be used to develop new or improved capabilities for protecting our nation from terrorism and its consequences. Some examples are provided below.

Confronting Weapons of Mass Destruction
The Office of Homeland Security has coordinated a major multi-agency research effort that will lead to improved techniques for timely detection of biological attacks on our nation, and for minimizing the consequences of an attack. In the Department of Health and Human Services and the Department of Defense (DOD), funding for bioterrorism R&D is increased from a pre-9/11 level of just over $300 million to more than $2.4 billion—more than a factor of seven increase. $1.75 billion is provided to the National Institutes of Health (NIH) to perform fundamental research leading to the development of rapid identification and monitoring technologies, diagnostic tests, new vaccines and therapeutics, including an improved anthrax vaccine. An additional $49 million would be provided to the Food and Drug Administration (FDA) for research and drug approval. Aside from a variety of other research activities, the DOD will dedicate $420 million to ensure rapid detection of biological agents, devise countermeasures, and to study and model the technology and tactics of bioterrorists. The Environmental Protection Agency (EPA) will receive $75 million to develop improved techniques and procedures for coping with biological and chemical incidents. Additionally, investments are being made to enhance the nation's capability for detecting the use of chemical and radiological weapons. The Department of Energy (DOE), for example, will demonstrate a multi-station prototype of a chemical agent detection and response system in the Washington, D.C. Metro system.

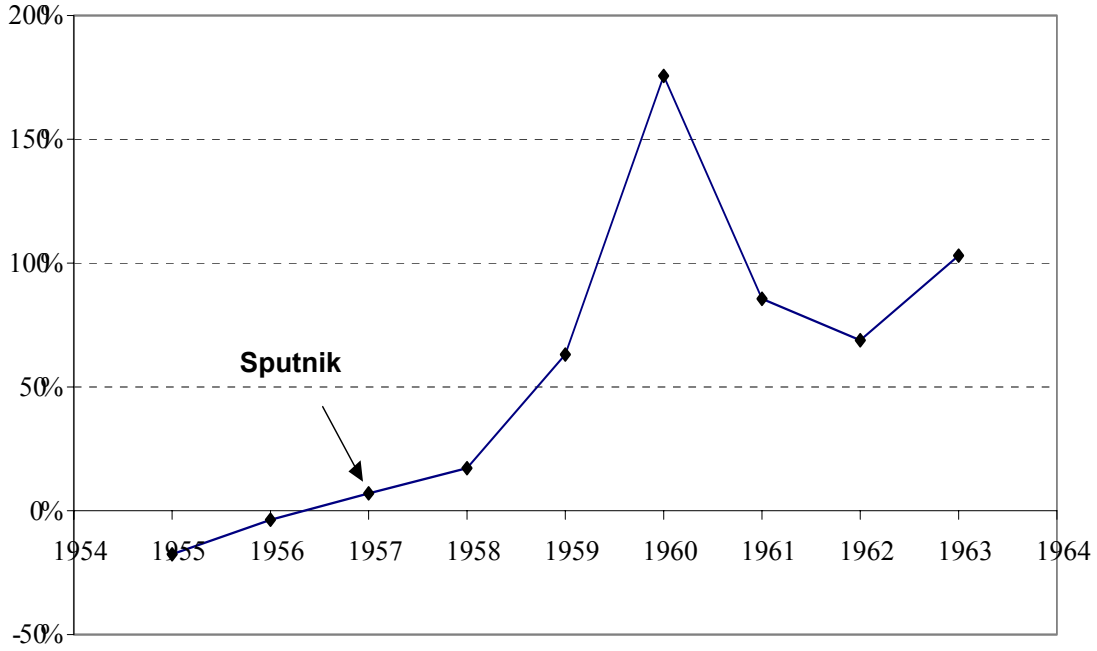
Detecting Potential Danger
A collaborative effort between the Department of Justice, the Federal Bureau of Investigations, the National Institute of Standards and Technology (NIST), and DOE will investigate the reliable identification of specific individuals, even when attempts have been made to alter appearance, by measuring the "biometric" signatures of people passing through, for example, airports. The effort will range from development of surveillance sensors to algorithms that interpret their data and automatically alert operators to potentially dangerous people.

Explosives Detection
The Federal Aviation Administration, DOE, and the Technical Support Working Group (jointly sponsored by the State Department and DOD) will research improved methods for detecting conventional explosives in luggage, in airports and other transportation portals, at the borders, and in high population density areas.

Setting Standards
There will be a coordinated multi-agency effort for setting appropriate standards in homeland security; these agencies include NIST, EPA, the Centers for Disease Control and Prevention, and the Nuclear Regulatory Commission. Areas of focus will include setting standards for equipment used by first responders, and setting decontamination thresholds for determining when an area can be reoccupied after an attack.

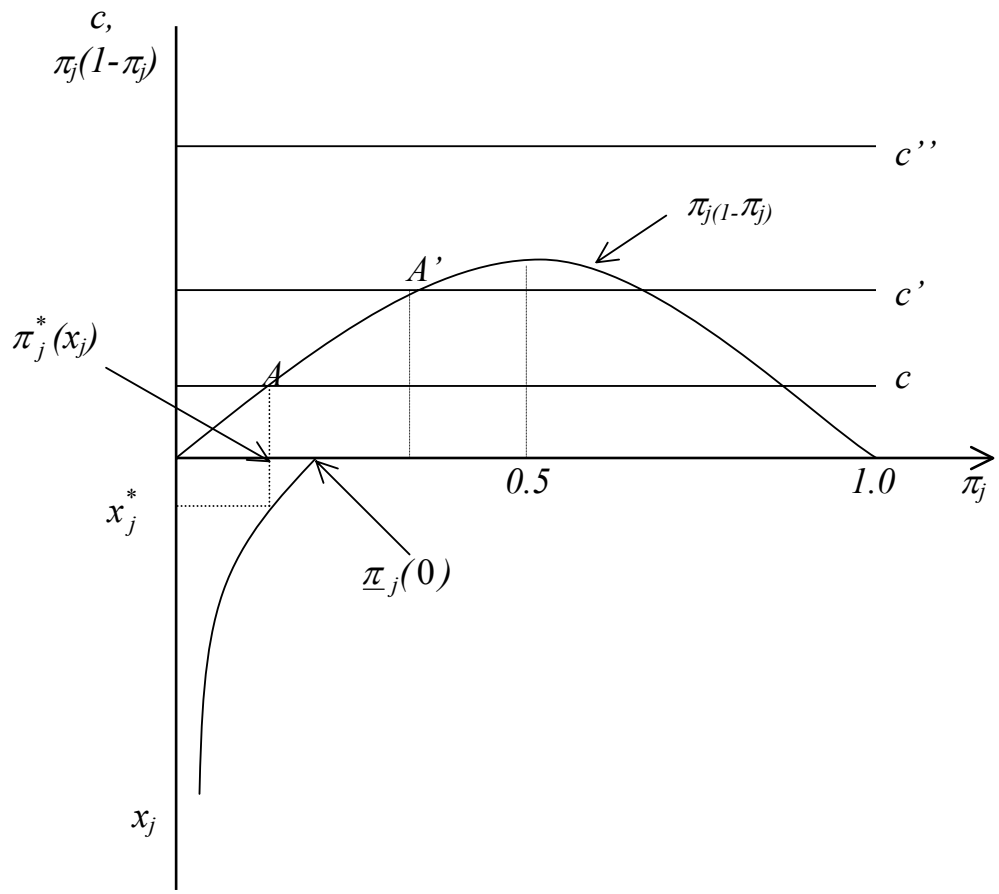
Basic Research
Fundamental investigative efforts will be funded at several agencies to provide basic scientific data for the war against terrorism. These efforts include $27 million for fundamental work at the National Science Foundation for sequencing the genomes of pathogens, so that more effective detection schemes and defenses might be developed, and work at NIH on developing candidate products that could become the next generation vaccines.

Figure 1
NASA R&D Expenditures
Yearly Percentage Changes: 1955-63



Source: Mowery and Rosenberg (1989), table 6.12, pp. 161-165.

Figure 2
The optimal level of private spending on security



$c = 1/\beta pL_j$

The optimal level of x_j: $x^*_j = arg\ \pi^*_j(x_j)$

$$\pi^*_j(1-\pi^*_j) = c \le 0.25, \quad \pi^*_j \le 0.5,^{37} \quad \pi^*_j \le \underline{\pi}_j(0)$$

[37] Because of second order conditions.