



Heiko Borchert

**It Takes Two to Tango – But Who Wants to Dance?
Engaging the Science and Technology Community
in the Fight Against Terrorism**

NATO Advanced Research Workshop
Science and Technology Policies for the Anti-Terrorism Era

PREST, University of Manchester
12-14 September 2004



Overview: Three Key Messages

- Engaging the S&T community requires a **comprehensive approach**
 - ⇒ Basic research and role of social and cultural sciences

- There are **normative, regulatory, economic, and scientific incentives and disincentives** that need to be addressed in order to tap into the expertise of existing and new S&T stakeholders

- There is an urgent **need for a more strategic approach** to security S&T at the national and at the European level in order to
 - ⇒ bridge existing gaps between foreign and security grand strategies and S&T strategies
 - ⇒ provide capabilities commensurate with the new security risks



Comprehensiveness is Key to Engage the S&T Community

S&T help us to

- **Understand** the nature of new risks, their causes and consequences
- **Improve** existing and define new strategies to deal with these risks
- **Provide** adequate capabilities to address the new risks at the national and at the international level

But

Given the nature of new security risks it is **important not** to focus on **specific disciplines** or on **singular risks alone** when discussing security-related S&T contributions (e.g., GoP Report, European Preparatory Action Plan for ESRP)

Thus

Comprehensive agenda needed to mirror a comprehensive understanding of security



Basic research and social and cultural sciences are as important as technology and product-related R&D



Incentives and Disincentives

	Disincentives	Incentives
<p>Normative domain Addresses the general framework within which security and S&T communities operate</p>	<ul style="list-style-type: none"> ▪ Conflicting values (secrecy vs. openness) can hamper cooperation ▪ A lacking sense of urgency among key stakeholders makes it difficult to launch actions 	<ul style="list-style-type: none"> ▪ Strong incentives for self-regulation to avoid ill-judged regulations ▪ Establish a new playing field for public-private interaction <ul style="list-style-type: none"> ⇒ Create experimentation environment (NITEworks)
<p>Regulatory domain Sets specific guidelines for S&T activities and thus influences decision-making</p>	<ul style="list-style-type: none"> ▪ Division of regulatory competencies can lead to unfavorable outcomes ▪ Lack of regulations (e.g., IP protection) is a reason for absence of industry activities ▪ Existing regulations can be too cumbersome for dealing with new security risks (e.g., approval processes) 	<ul style="list-style-type: none"> ▪ Beware of quick fixes of regulatory issues ▪ Comprehensive approach is needed to take into account general economic considerations <ul style="list-style-type: none"> ⇒ Multinational companies influence R&D structure ⇒ Preferences of banks and need for VC



Incentives and Disincentives

	Disincentives	Incentives
<p>Economic domain Addresses the business logic for S&T communities to enter into new markets</p>	<ul style="list-style-type: none"> ▪ Diverging profit expectations ▪ Increase of funds could aggravate security problems (because of an increase of people working in critical sectors) 	<ul style="list-style-type: none"> ▪ Create a market <ul style="list-style-type: none"> ⇒ US BioShield ▪ Stimulate R&D and increase manufacturing capacities <ul style="list-style-type: none"> ⇒ US BCR Weapons Counter-measures Research Act ⇒ DARPA ▪ Address legal risks <ul style="list-style-type: none"> ⇒ US Homeland Security Act transfers litigation risks to the government
<p>Scientific domain Addresses the scientific logic for S&T communities to enter new fields of activities</p>	<ul style="list-style-type: none"> ▪ Fear of ensorship due to national security concerns ▪ Individual curiosity could deter scientists from near-term product-related research 	<ul style="list-style-type: none"> ▪ Do not overestimate risk of censorship ▪ Governments must create long-term conditions (e.g., steady flow of funds, experimentation environment)



Outlook

Map Existing Capabilities

- Joint working groups should identify existing S&T needs with regard to security- related activities and assess national S&T capabilities

Develop Security S&T Policy

- Bridge gap between grand strategy and S&T strategy by defining security S&T strategies ⇨ key to support the implementation of the ESRP
- "Office for Security S&T" to provide strategic guidance and to coordinate procurement and offset programs, S&T activities, and industrial policy

Harmonize Capability Development and Security S&T

- European security S&T policy should cut across existing policy areas
- European Defense Agency should consider programs for emergency responders and should expand its steering board to include non-security S&T stakeholders

Launch S&T Diplomacy

- Complement foreign policy portfolio with tailored S&T activities, i.a. to improve self-regulation and promote confidence-building