

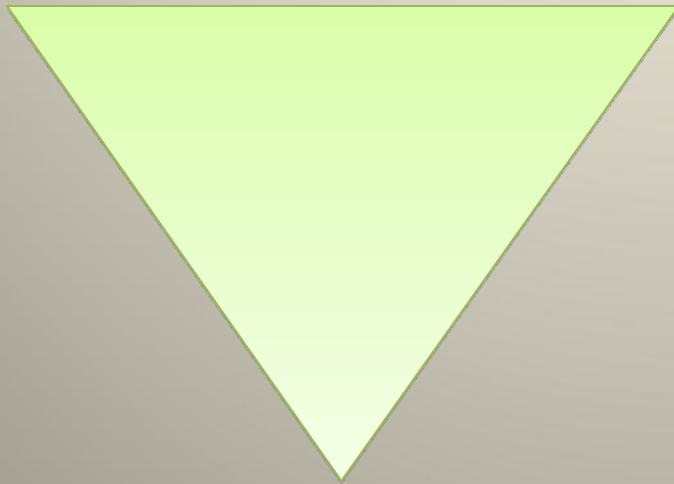


RUSI 4<sup>th</sup> Annual S&T Conference for Homeland  
Security and Resilience  
25 June 2008

A year in reflection

Sir David Omand GCB

Visiting Professor, Department of War Studies,  
King's College London

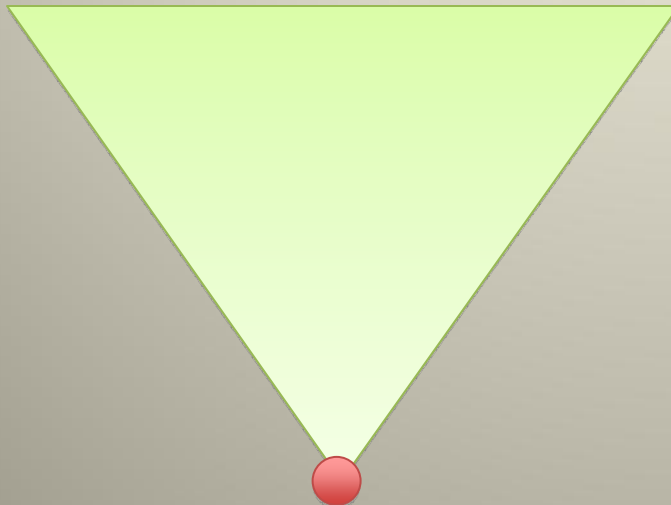


Emergence of National  
Security Strategy

Bedding down on  
OSCT in the Home  
Office

# Emergence of National Security Strategy

Three strategic principles



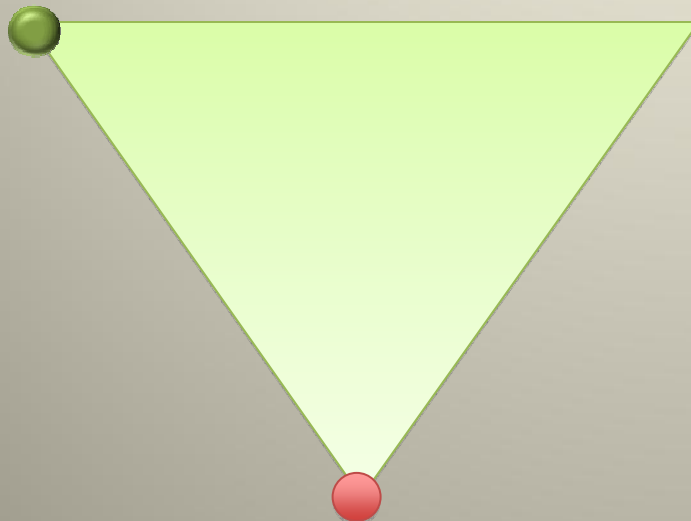
**Adopt a citizen  
focus  
'human security'**

Helping create confidence that the major risks facing people at home and when abroad are being managed satisfactorily – covering Hazards and Threats

So that people can live their normal lives, freely and with confidence,

# Emergence of National Security Strategy

**Apply  
anticipatory  
policies**



**Adopt a citizen  
focus  
'human security'**

Working on likelihood,  
vulnerability and impact

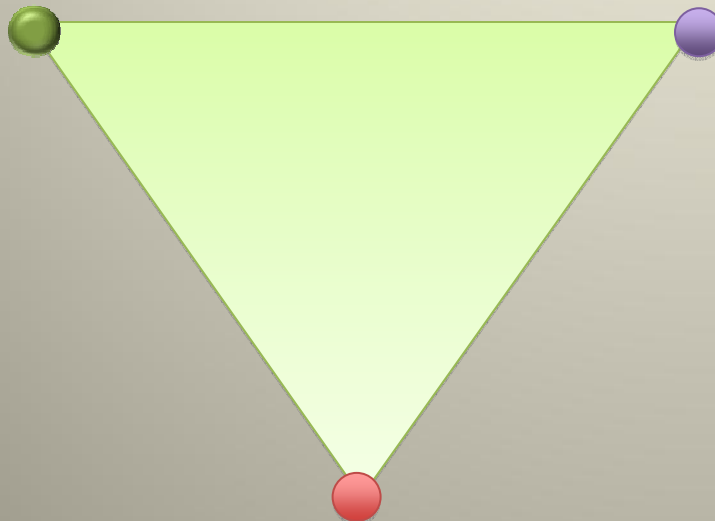
Domestic and overseas

“Responsibility to  
protect”

Importance of  
intelligence

# Emergence of National Security Strategy

**Apply** **Build**  
**anticipatory** **overall national**  
**policies** **resilience**



**Adopt a citizen**  
**focus**  
**'human security'**

Greater vulnerability of advanced societies

Critical National Infrastructure protection

Psychological dimension of resilience

Risk management approach

# Emergence of National Security Strategy

**Anticipatory policies**      **Building overall national resilience**



**Citizen focus  
'human security'**

CT Strategy firmly embedded within National Security Strategy

CONTEST – refreshed

Long term S&T requirements

## Are we looking sufficiently far ahead?

- Developments at network, cell and individual level
- How the internet is changing their communication reach
- The way that modern media gives their actions immediate impact, so targets do not have to be in London
- Suicide tactics and the impact on investment in protective security measures
- Millenarian ideologies making CBRNe more likely

## Is 'detection' technology and methodology improving in practice?

- The location, operations and aspirations of suspected terrorists
- Their modus operandi for attacks
- The communications, logistics, training and financing of their networks
- Target selection and reconnaissance and activities
- The identity of potentially dangerous extremists in our societies, either as actors or facilitators
- The movements of suspected terrorists
- Recruitment activities
- Mutations, developments and fissures in the threat

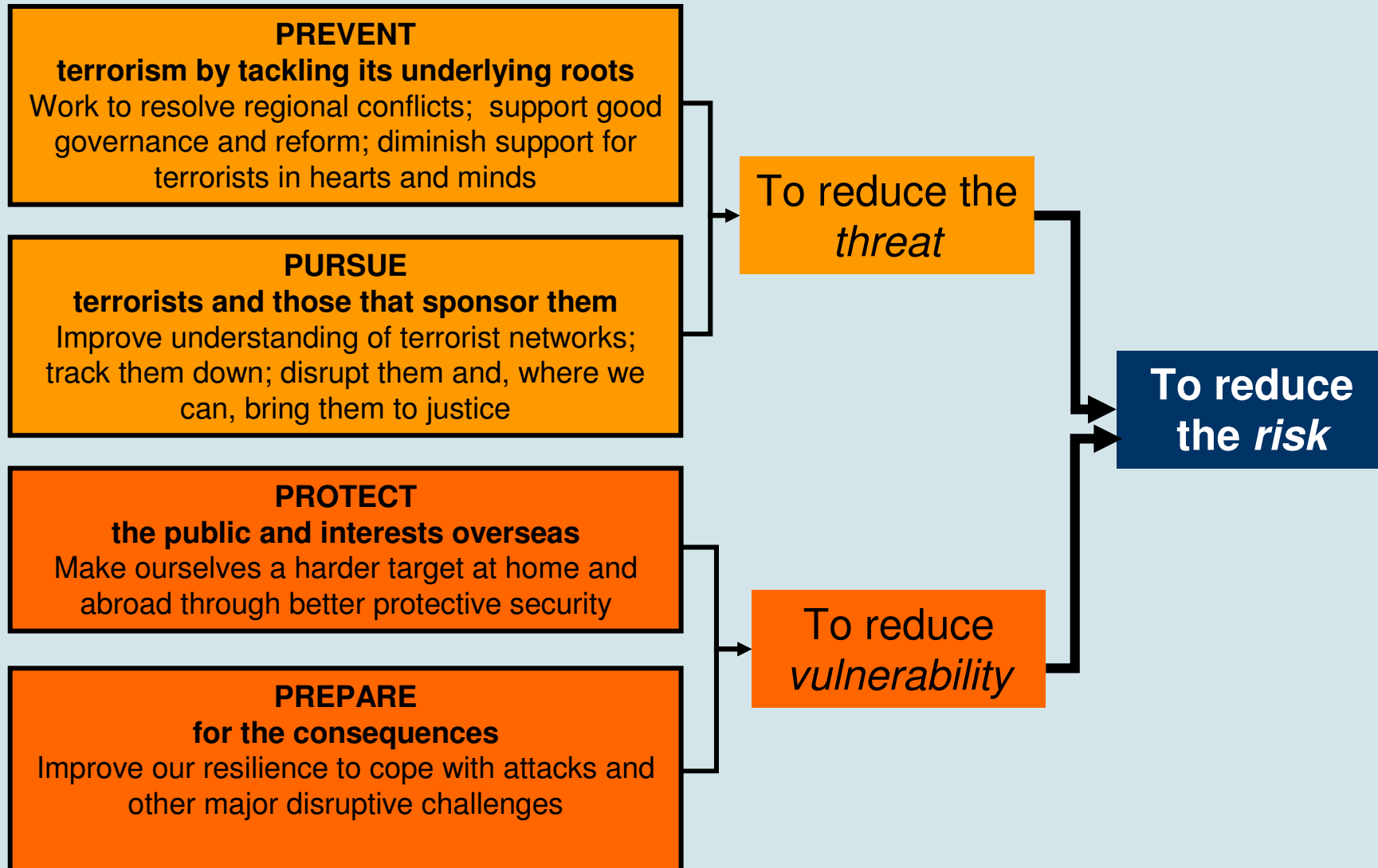
## Do we have a better handle on who we are trying to detect, and how?

- A core of activists: experienced and trained AQ-related terrorists, able to inspire, plan and mount complex terrorist attacks
- Radicalised individuals prepared to provide practical support, financing and at times are able to conduct criminal acts of terrorism of their own through informal networks
- Those who operate 'gateways'; finding those who follow the intolerant extremist 'cult' ideology - a world-view backed by a powerful and graphic narrative of religious righteousness and victimisation, widely accessible through the internet
- Those who may provide extremists access to CBRNE means
- Those who may seek to copy terror tactics for other causes

## Do we have a better understanding of what we are trying to prevent? AQ strategy

- Ends: religion and state unified under Shari`a over all Muslim lands, free of Western influence (Caliphate)
- Ways: weaken enemy, build strength, return to local fights
  - Cast the US, Israel and the West as the 'crusading' and invading enemy (culturally as well as militarily)
  - Diminish the perceived power of the US and allies forcing their retreat, thus reducing their ability to frustrate Islamist revolution
- Means: extreme terrorism to expose weakness of the West, and to create revolutionary consciousness of Ummah with sense of personal duty to join the 'defensive' struggle

# Delivery of campaign plans: but against what timescale and threat?



## Deploying resources as part of a coherent security strategy

- Keeping terrorism in proportion: one of the risks of the 21<sup>st</sup> century to be managed in a national security strategy:
- Pursue all 4 'P's in cooperation: Prevent, Pursue, Protect and Prepare
- Infrastructure programmes : immigration and borders, passports, identity, passenger and cargo screening, CCTV, ANPR, radiological detection, and ??
- The goal is security: a state of confidence that the major risks to individuals, families, communities and businesses are being adequately managed so that everyday life can continue

## Deploying resources as part of a coherent security strategy

- Where is the single security budget? How does government organise horizon scanning?
- Lessons from the last year: water, power, fuel etc. Balance investment across the risk = reducing likelihood x vulnerability x impact.
- Minimax and Maximin defensive investment: both required
- Role of regulators of the CNI
- Balance investment for present threats and for future, eg Olympic legacy
- Harness all of our strengths including technology: using the RISC framework for new level of engagement with industry

## Review of Home Office Science Findings of the Chief Scientific Adviser

- the need for a strategic approach;
- effective management of science;
- joint working (both across disciplines and stakeholder groups);
- overcoming the obstacles to the use of science;
- publication and knowledge transfer; and
- use of external scientific advice and expertise;

## Relevant technology 'clusters'

Security

Sensors

Networks

Nanotechnology

Information technology

Energy

Body/mind

Advanced materials/robotics

The logo consists of the word "RISC" in a bold, white, sans-serif font, centered within a dark blue rounded rectangular box. The background of the entire slide is a light gray gradient with a dark blue line that runs horizontally across the middle and has diagonal segments at the top-right and bottom-left corners.

**RISC**

## RISC is an alliance of:

- suppliers
- trade associations: BSIA, DMA (inc APPSS and NBC(UK)), Intellect, SBAC
- think-tanks (outreach to academia)
- It provides a channel of communication with Government on strategic issues affecting national security and resilience. This enables unprecedented Industry-Government partnership and dialogue to counter international and domestic terrorism.
- Over 2000 companies or 80% of the supply base are represented through its trade association members, from prime contractors and global leaders through to Small and Medium Size Enterprises (SMEs) and start-ups.



## **RISC's aspirations:**

- **Help make Britain's defences more versatile and agile.**
- **Help better pull-through of technology from industry**
- A long-term relationship between RISC and Government that will yield knowledge of capability that is needed - today and tomorrow.
- Reducing the time it takes to move from identifying new problem-solving technology to getting it into the field.
- Government and supply community understanding each other better and improving co-operation
- Filling the capability gaps that exist - in advance of, and not after, attacks are launched.



## **RISC and Government: work in progress**

- Industrial Advisory Groups

- April: first groups being launched in key sectors

1) CBRN □ 2) ICT □ 3) Standoff detection from suicide bombers □ 4) Critical National Infrastructure Protection

1) Other issues being examined include: joint work on horizon-scanning; international co-operation including UK involvement in EC Framework 7 projects on security; US Safety Act and implications for industrial liability in the UK

## **RISC next steps**

- For further information on RISC, please contact:

Derek Marshall

[derek.marshall@sbac.co.uk](mailto:derek.marshall@sbac.co.uk)

020 7091 4517

