http://www.lensforum.com/

Summaries & Findings

1. Introductory Presentations

2. Common Security Needs

3. Partnerships and Expectations

4. Establishing and Co-ordinating Partnerships

5. Tangible Benefits for Potential Contributors

6. Intelligence Oversight and Organisation

10. In his opening address, the Chairman highlighted the fact that our economies and societies were increasingly dependent upon a seamless and borderless connectivity through networks spanning the entire globe. However, the benefits of integration went hand-in-hand with the vulnerabilities that were always there. How these, as well as the other challenges brought about by globalisation, were managed would at the end of the day decide the fate of the current (third) phase of global development. In meeting the more long-term threats to global security, it would be necessary to provide defence in the form of forward-looking global policies. Simply to react would not be enough; prevention would be the true road to stability.

11. It was clear that broad security issues could no longer be left just to governments. Although the ultimate responsibility was theirs, it was truly a public-private partnership that was required and one in which business had a large and important role to play. Today, more than ever, security must be an integral part of all activities, whether in business or elsewhere. There would be a need to balance costs, risks and effectiveness in an endeavour that would be not only difficult to manage but also open to constant debate. Thus, statesmen would need to develop a concept of forward defence in the form of forward-looking global policies as well as ones which ensured that security was smart and seamless, not suffocating and senseless, click for details.

12. The former Chairman of the UK's Intelligence and Security Committee stated that the requirement of democratic societies in the modern security environment was not only to raise people's awareness of the serious nature of the new threats but also to recognise that these threats should be met by positive action and not by panic. It was vital that the public had confidence that there was a coherent strategy to tackle the current challenging situation. In defeating terrorism, the first and obvious challenge was to tackle basic grievances that fuelled so much of the terrorist's motivation. Here, the winning of 'hearts and minds' was essential and modern communications - with balanced reporting - had an important role to play in this regard. A second challenge was to ensure better co-ordination of our intelligence and security agencies in order to forestall future outrages. What was also needed in any assessment was much more imagination and lateral thinking in anticipating the types of threats that may emerge. The third critical requirement was to deny the terrorists the cash that they require to resource their activities; it was believed not enough had yet been achieved in this area. A fourth challenge was to introduce new legal powers while ensuring that these did not conflict with present attitudes on civil liberties, click for details.

13. In an assessment of the impact of economic security on business, the Secretary General of the International Chamber of Commerce expressed a view that efforts to achieve better security did not result in a sharp fall in business competitiveness or efficiency. The criteria which directed the needs of commercial activity was not necessarily compatible with those of general security, and countries should be aware of the wider impact of some seemingly straightforward security legislation. The searching of increasing volumes of container traffic and growing travel delays through detailed searches at airports were just two examples of how better security could

potentially hinder commercial activity. Also, it was pointed out that restrictions on the migration of qualified people for security reasons could also have a deleterious effect on wider economic development.

14. In general, the business world had readily adapted to new circumstances and had usually been better than governments at developing new technologies to address new challenges. Furthermore, the open exchange of data would be a key part of facilitating international commerce in the light of trends in globalisation and security. It should also be remembered that for the majority of businesses, terrorism was not the number one priority in risk terms. It was therefore up to governments to find an appropriate balance between the different security measures designed to prevent acts of terrorism and those which allowed the legitimate needs of a commercial world to continue with the minimum of disruption, click for details.

Common Security Needs

15. Three fundamental threads were examined by different speakers in an attempt to uncover the essential drivers which would influence security policy in the future. Two of the presenters focused on extremism (in the form of terrorism and fundamentalism) while the third provided an insight into how technology could not only have beneficial consequences but also presented risks of its own.

16. In his assessment of the future of political violence, the Director of RAND concluded that terrorism would remain instrumental and that all democratic societies would remain vulnerable as the fundamental asymmetries in international politics were the terrorists' appeal. Terrorism was a perennial, ceaseless struggle designed to undermine confidence in both government and leadership. The enmity towards the US and other democracies was unlikely to diminish from the terrorists' manifesto. In this regard, the conflict was never-ending, yet to speak of a 'war' implied finality, click for details.

17. This theme was continued by way of a key-note address by the Special Adviser on Homeland Security to the US President. He emphasised the need to bring the battle to the enemy through preventive and pre-emptive strategies. He outlined the three priorities of the US national risk management plan: win the war abroad, secure the homeland, and secure and revive the economy. In the last of these, he saw a major role for business and the need for partnerships in the public-private sector. The creation of a Department of Homeland Security, bringing together 170,000 employees, was an attempt to make the sum of the parts greater than whole. In questions, certain members of the audience raised issues over introducing another layer of bureaucracy and the importance of winning 'hearts and minds' in addition to battles, click for details.

18. In an address on the wider aspects of governance, the former Chairman of the UK's Joint Intelligence Committee made the point that Western democracies were subject to powerful centrifugal forces which strained traditional bonds and made them vulnerable to fragmentation and alienation. The transplantation of this model around the world, with little time to mature in local conditions, had loosened local bonds without necessarily replacing them with democratic structures. It had been met with very partial success, and was widely undermined by autocracy and corruption. Threats to Western security were acute where religious fundamentalism - formerly exploited by Western and local governments to combat Communist and left-wing forces - were exploiting the weakness of failed states and hatreds engendered by local conflicts to terrorise their erstwhile patrons. Military responses would be unavoidable but insufficient to provide long-term security, click for details.

19. The range of security threats to our information infrastructure, as well as the inherent weaknesses associated with the underlying technology, was highlighted by the Head of Information Security at Consignia. The speaker stated that in spite of inherent weaknesses, security technology would help to transform business and that IT security was beginning to influence management agendas. Most people overestimated what would happen in the next three years and underestimated what would happen in the next 10 years. The critical period would be 2005-06 when several key technological trends peaked or matured. Surviving this period would require a

step change in electronic security, and road mapping could be used to help identify drivers, trends and requirements, click for details.

Partnerships and Expectations

20. All the speakers addressing the question of partnerships and stakeholder expectations made the point that 'people, process and technology' were all essential and inter-linked components in determining security. Like a three-legged stool, all the legs must remain of equal length if the stool was to remain upright. When one or more legs fell short then the stool was likely to topple.

21. In a key-note address, the Chairman of the Police Information Technology Organisation stressed that the globalisation of commercial enterprises and corporate downsizing had led to an increasing dependence on technology to sustain shareholder value and business benefits. Those with limited resources struggled to 'pick the winners', conscious that their decisions would shape the future of their business. Similar choices faced those responsible for law enforcement and national security. International collaborative benefits included shared knowledge, shared costs, shared technology, interoperability and improved capability. The critical success factors were corporate commitment and leadership, development of concepts and doctrine, and phased funding. He was pleased to see the police designing and adopting a doctrine for the future, click for details.

22. Three separate presenters examined the requirements of law-enforcement agencies, the business sector, and the military. In addressing the first of these, the former Chief Constable of Merseyside stated that while the agencies involved did consult, collaborate and co-operate, they all had their own legislative and constitutional base from which to operate. Culture, competing interests, rivalry and protection of 'turf' were undoubtedly strong elements. However, as it had proved difficult to overcome many of these traditional issues within nations, the idea of still greater centralisation or internationalisation in the fight against transnational threats was hard to visualise, click for details.

23. In his vision of the business sector, the Chief Executive of QinetiQ said that for much of business security was of nil-benefit cost but that security failure could be catastrophic. He developed the three prongs of security (planning, people and physical). In planning, he emphasised the need for a vulnerability assessment based on consequences and costs, while he reinforced the message that people were often the weakest link in any security apparatus. The physical aspect was the cornerstone of most security environments and the one that brought together high-integrity solutions. By introducing a fourth (cyber) dimension, the speaker addressed how critical resources could be safeguarded through trusted information management systems such as the Public Key Infrastructure. Security was a field where both technology and methods were quickly developing, with many initiatives transferred from the military sector, click for details.

24. The Special Adviser on Central and East European Affairs to the Office of NATO Secretary General made the point that defence and security were no longer synonymous. Today, security included defence but it was now a concept which had a much wider remit. And while we were all facing the same international threat spectrum - organised crime, illegal migration, terrorism, ethnic strife, etc - we faced them in a different order of priority. Hence, although the threat may be common, the responses had to be different, even within the members of NATO. Also, with the abolition of the distinction between peace and war in the modern age and a new interpretation of deterrence, the differences between internal security and external security had been lost and hence so had the functions of the military and the police. Yet the right mix of forces, the right level or degree of collaboration between agencies, or the right level of contingency planning had been so far absent to any substantial degree. It was argued that much more thinking was needed if an adequate response was to be formulated, click for details.

25. In parallel workshops, two key problem areas were studied in detail. One examined how it may be possible to break the financial link between crime and terrorism and defeating. An Associate Director with TRANSCRIME offered an insight into how instruments such as financial legislation

and anti-money-laundering regulations could help reduce acts of terrorism in a preventative way. The harmonisation of policies across the EU was reviewed and the significance of such policies was considered against the financial background of the 19 hijackers from 11 September, click for details.

26. In a separate workshop, two principal consultants from Anite and QinetiQ considered how attacks against information networks could be defeated. The speakers recognized that people formed the basis of information networks whilst IT was the supporting structure. As a result, it was likely that what constituted the defeat of an attack for one person (or group of people) may not be the same for others. Indeed, the perception of an attack could also vary and much would depend on organisational strategy and motivations. It was emphasised that in response organisations needed to develop long-term strategies and promote best practice while governments needed to provide incentives for information sharing and consider improvements in legislation. A pro-active approach could only come about through the good use of resources and where security became a core competence. Clearly, commercial organisations should develop their own form of intelligence networks and look beyond their own boundaries when developing security strategies, click for details.

Establishing and Co-ordinating Partnerships

27. In attempting to answer the question as to how long-term partnerships can be established and co-ordinated - locally, nationally and internationally - in the face of diverse threats and varying priorities, three speakers examined the ways in which risks, intelligence and ownership could be shared.

28. In the case of risks, the Vice President (Europe) with Pinkerton portrayed the government/corporate responsibility relationship as one which fluctuated according to the issues. In the case of intellectual property theft, fraud and 'aspirational' counterfeiting, business tended to lead - and demonstrated high levels of capability - in tackling the problems while the concern of governments was relatively low and expressed through legislation and corporate-governance regulation. Governments and business tended to take equal share over topics such as organised crime, kidnap and ransom, and 'expectational' counterfeiting. However, governments clearly adopted the lead and showed greatest concern - while business took a lower capability profile - when tackling conventional and extreme-impact terrorism, click for details. The comment on the level of risk from terrorism within business was made earlier by the Secretary General of the ICC.

29. In his address on sharing intelligence, the Deputy Director of Europol stated that the events of 11 September 2001 had forced all those within intelligence and law enforcement to re-assess fundamentally the way knowledge and intelligence products were shared with each other and with other parts of government. In order to facilitate this process, Europol had employed two procedural techniques: first, the use of a standard evaluation criteria in order to test the veracity of information; and, secondly, the use of handling codes on this material to facilitate its exchange and dissemination. However, if sharing was to be effective people needed to trust information with other organisations, knowing that only by sharing would come added value without the loss of data integrity, click for details.

30. The issue of trust was a feature that permeated the subsequent presentations from the Head of Security at BAT. He stated that trust was a risk condition. Success in partnerships could be assured through winning 'hearts and minds', implementing a co-ordinating body with a focus-point infrastructure, ensuring communication not only worked but was also inclusive and involved 'satellite' dissemination. While there were models to follow, the question of who pays for such facilities was important. He concluded that the development of ownership could come about through 'forming, storming, norming and performing', click for details.

31. In parallel workshops, the question of whether partnerships could work more effectively was examined in the defence and insurance markets. In his address on the defence industry's involvement in focusing on the new security challenges, the Vice President (Civil Affairs) at the

Lockheed Martin Corporation made the point that since 11 September over 12,000 defence industry capabilities in the US had been identified as being of value in the fight against terrorism. The fundamental issues were: trusted field-level policy enforcement, trusted third-party secure information management, sharing appropriate information while protecting sensitive data, and implementing full audit trails. The solutions were both immediate and longer term, the latter coming through an overarching ('enterprise) architecture which would provide a framework for legacy-system interoperability. However, in the final analysis, technology was not the issue but bureaucracy was, click for details.

32. The speaker from Catlin Underwriting Agencies (Lloyds of London) addressed the difficulties of the insurance market after 11 September. While terrorist cover on major (iconic) buildings and downtown aggregations would remain a problem, there were also difficulties with certain countries due to the perceived political risks (war, embargo, inconvertibility of currency, etc). However, it had been possible in a co-ordinated effort with the World Bank to assist certain African countries through an alliance of concerned parties. Such alliances had benefits for the policy holder (through better cover, cheaper rates and longer periods), the risk country (through increased trade flows) and to the insurer (through risk migration). It was therefore important to continue to examine new structures and partnerships in efforts to overcome market inadequacies, click for details.

Tangible Benefits for Potential Contributors

33. The focus in answering the final question on tangible benefits was on IT networks and protecting national infrastructures. Three technical experts attempted to provide answers by taking - in turn - business, a national-security and e-government perspectives. The Group Security Director of BT stated that business should help the common cause because customers wanted secure and survivable supplies, governments wanted resilient companies, while businesses wanted to reduce their insurance costs and comply with legislation. It was clear that good security was a business discriminator which would help to enhance trust and retain both a customer and shareholder base, click for details.

34. The senior representative from the US National Communications System emphasised that in the wake of 11 September the USA could not act alone, either within borders or outside of it, because much of the infrastructure was neither owned nor operated by the government. This formed the basis of a need to partner with the private sector, namely the telecommunications industry, and to craft appropriate protection and response mechanisms. Similarly, the impact of globalisation upon that infrastructure, and the economic issues related to it, had impacted on how and when one could and should respond. At the heart of the National Security and Emergency Preparedness (NS/EP) telecommunications environment was a strong partnership between industry and both the defence and civil sectors of government. This partnership had continued for 19 years in the US and was frequently cited as the model for industry/government co-operation on infrastructure issues. The key challenges for the future were: to link up key government and industry sites, develop information-sharing mechanisms (processes and technologies) to protect sensitive information, and advance NS/EP programmes to keep pace with converging technologies. The benefits would be greater security for all, click for details.

35. In considering e-government, the Head of Infosec at the UK's Communications-Electronic Security Group (CESG) reinforced once again the importance of combining people, systems and technology within a sound policy framework. This policy had also to be underpinned by trust. A partnership between the UK's E-Envoy and CESG had emerged in the form of the Public-Key Infrastructure (PKI) Trial. To date, PKI had a slow take-up in government and it had been necessary to build up confidence in this technology and to ensure that commercial vendors could provide interoperable solutions. However, the benefits of improved interoperability, better competitive tendering and international spin-offs were all beginning to appear. The trail was reported to have been an unqualified success and was claimed to be a world leader for both government and vendors alike, click for details.

Intelligence Oversight and Organisation

36. In a key-note address on the political control of intelligence and intelligent agencies, the Liberal Democrat Foreign Affairs Spokesman said that the British practice of intelligence oversight needed to be re-examined for two reasons: first, the public must be able to be confident that the security services were prepared; and, second, the threats facing the UK and its allies would benefit from more open access to intelligence-related products. The speaker advocated a fully constituted Select Committee (along the lines of the US system) which could hear evidence from a range of experts instead of purely from agency staff, as was the current practice with the Intelligence and Security Committee. In this way, parliament would have a role as both investigator of, and advocate for, the intelligence services. A stronger legal and political basis for the security services would allow them to be more judicious in their application of classifications and more able to assess the full spectrum of threats and possible responses, click for details.

37. The Corporate Intelligence Adviser with Shell said that the company had devised a three-tier approach to developing its intelligence capabilities based on people, process and technology. Such an approach helped to leverage its culture of inter-personal relationships and trust in order to secure the maximum benefit from its various communities of practice that drove its intelligence network. Through recent organisational reforms, the company had harnessed and integrated a number of interrelated functions so as to utilise its knowledge in a more co-ordinated and effective manner, click for details.

38. The Director of Security and Privacy with EDS highlighted the need to focus attention on Internet security and the acts of cyber-criminals. Over 15,000 computer attacks were recorded in the first quarter of 2002 (compared to six in 1988), with the theft of information and financial fraud showing the highest increases. While 78% of large businesses suffered security incidents in a recent survey, 59% of the same businesses spent less that 10% of their IT budgets on information security. Hence, expenditure needed to increase by at least five fold, and possibly up to 10 fold, in order to produce realistic counter-intelligence measures. In the view of the speaker, success required: defined security and business objectives, tried and tested technologies, and scaleable and flexible systems. Areas to be developed in the future included cyber-forensics and biometrics, click for details.

39. In examining the role of business intelligence in fighting corruption, the Director of Forensic Services at Deloitte & Touche stated that financial crime was evolving rapidly and hence investigators and regulators needed to improve risk assessments and enhance due-diligence procedures. Employing business intelligence was not simply a check on specific individuals but included wider issues such as political links, procurement of assets, company track records and business ethics. In providing defences, there was clearly a need for more information sharing and more co-operation between authorities. Data protection and privacy legislation could be both a help and a hindrance in anti-corruption efforts, click for details.

40. A model for intelligence and security management involving public- and private-sector collaboration was used to assess some aspects of the previous speakers' points through group discussion. The SATELLITE (Strategic Corporate Intelligence and Transformational Marketing) model was designed to advance a more universal acceptance of the term 'business intelligence' in an effort to link intelligence gathering and knowledge enhancement. The model could be used to develop appropriate organisational intelligence systems, as well as analyse and interpret complex business issues, click for details.

41. The Director of IBM's Institute for Knowledge Management made the final presentation to the Forum with an eloquent description of how we assess and respond to problems and threats through pattern recognition. Much our response is based on traditional culture perspectives which tend to inhibit our awareness of other, more significant issues. By offering a model (the 'Cynefin' model) for pattern recognition, the speaker offered four different perspectives for problem solving. Using these perspectives, it would be possible for decision-makers and analysts, whether in

government, defence or industry, to conduct a step change in their strategic thinking. Further details of the Cynefin model are soon to be published by IBM, click for details.