Education Science & Technology for NATIONAL SECURITY

US National Security Agency

including Report of **Condaleezza Rice**

Former US Secretary of State during Bush Administration

Global Surveillance of United States & Reforms for National Security of Pakistan

Speaker : Engr Prof Adnan Haider , PhD

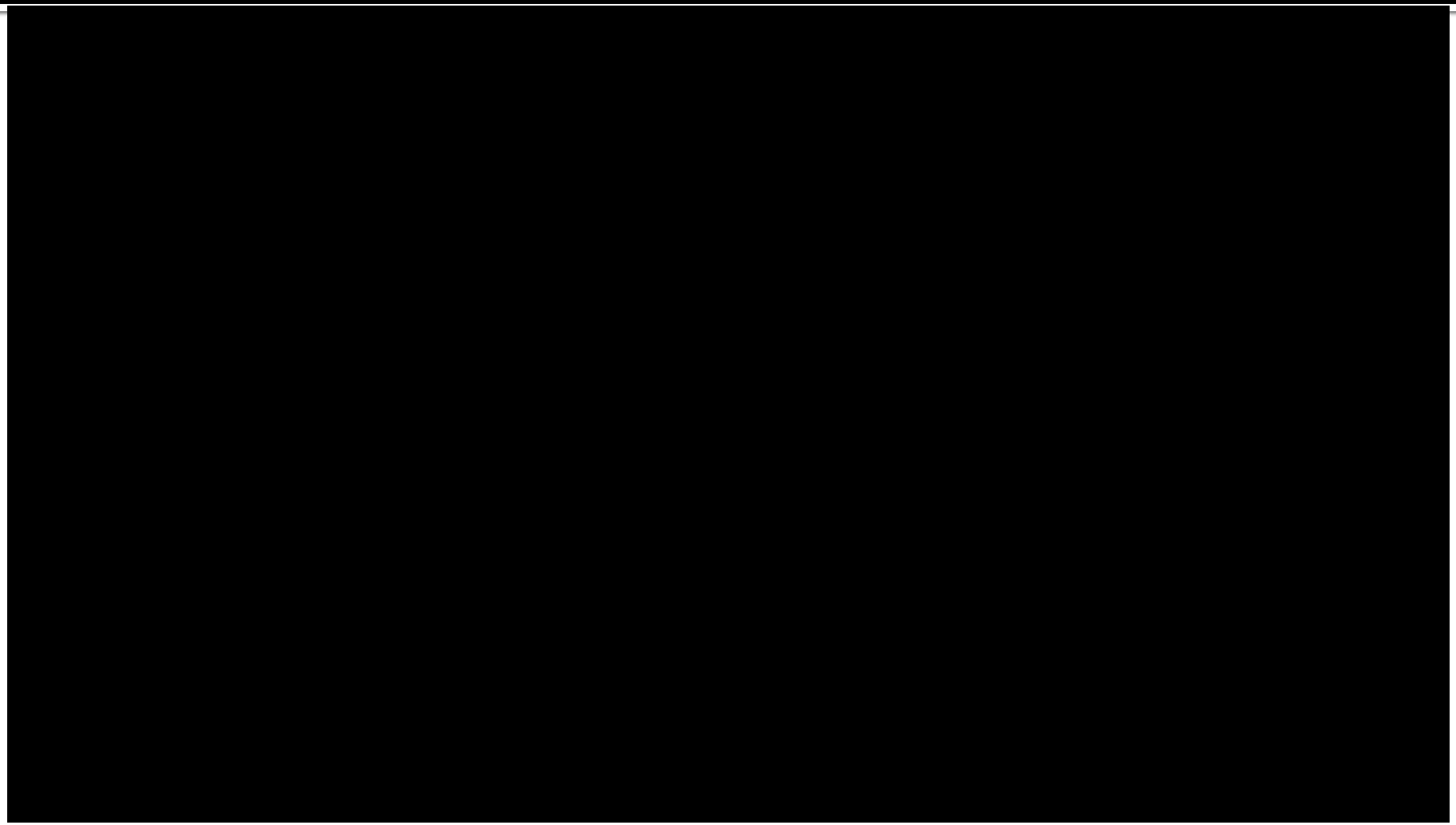
Post Doctorate Harvard University, MS, PhD New York State University

Scientific Advisor –

Race for Hillary Clinton –IADC Committee for US Presidential Elections 2016

Professor ,Chairman Strategic Planning ,Analysis & Review Cell, Chairman EE Dept

University of Management & Technology , Lahore



ELEMENTS of NATIONAL SECURITY

- Military security
- Economic security
- Resource security
- Border Security
- Demographic security
- Disaster security
- Energy security
- Geostrategic security
- Informational security
- Food security.
- Health security
- Ethnic security
- Environmental security
- Cyber security
- Genomic security

Education Reform and National Security of United States

Independent Task Force Report No. 68

- Joel I. Klein and Condoleezza Rice, Chairs
- Julia Levy, Project Director .

Education Reform and National Security of US

America's failure to educate is affecting its national security.

- Despite sustained unemployment, employers are finding it difficult to hire Americans with necessary skills, and many expect this problem to intensify.
- For example, 63 percent of life science and aerospace firms report shortages of qualified workers.
- In the defense and aerospace industries, many executives fear this problem will accelerate in the coming decade as 60 percent of the existing workforce reaches retirement age.

Education Reform and National Security of United States

- Most young people do not qualify for military service. A recent study on military readiness found that 75 percent of U.S. citizens between the ages of seventeen and twenty-four are not qualified to join the military because they are physically unfit, have criminal records, or have inadequate levels of education.

Education Reform and National Security of United States

- The 25 percent of students who drop out of high school are unqualified to serve, as are the approximately 30 percent of high school graduates who do graduate but do not know enough math, science, and English to perform well on the mandatory Armed Services Vocational Aptitude Battery.

Education Reform and National Security of United States

- The U.S. State Department and intelligence agencies are facing critical language shortfalls in areas of strategic interest. Fewer than half of State Department officers in language-designated positions in Iraq and Afghanistan met the department's language requirements, for example, and shortfalls in strategically important languages such as Chinese, Dari, Korean, Russian, and Turkish are substantial

Condaleezza Rice pointed out

- Implement educational expectations and assessments in subjects vital to protecting national security.
- Make structural changes to provide students with good choices.
- Launch a "national security readiness audit" to hold schools and policymakers accountable for results and to raise public awareness.

PART II

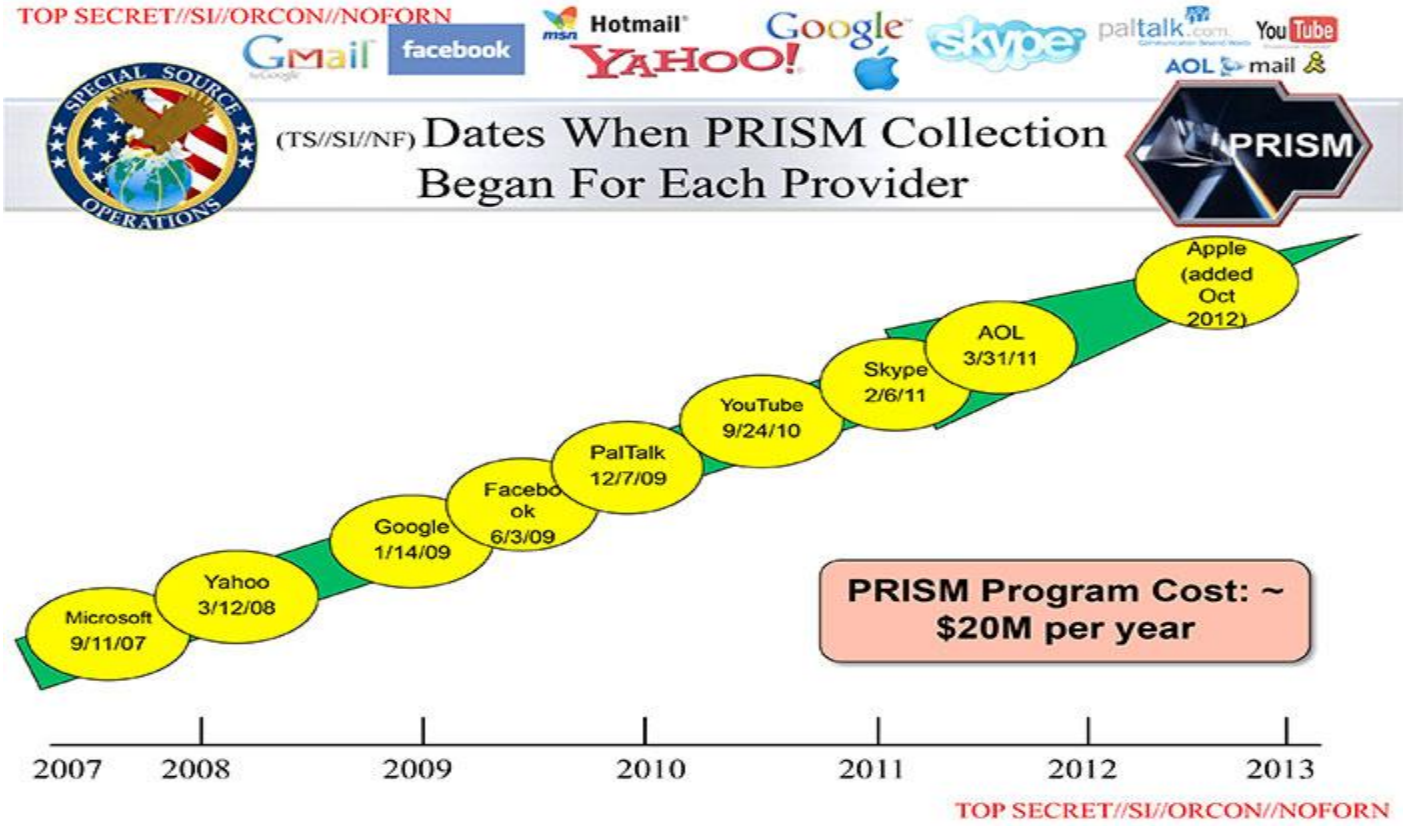
- TECHNOLOGY & National Security
- Examples of US NATIONAL SECURITY AGENCY's Technology and Systems

Global Surveillance Systems

- **XKeyscore** or XKEYSCORE (abbreviated as XKS) is a formerly secret computer system first used by the United States National Security Agency for searching and analyzing global Internet data, which it collects on a daily basis.

PRISM

- **PRISM** is a clandestine surveillance program under which the United StatesNational Security Agency (NSA) collects internet communications from at least nine major US internet companies.



ECHELON,

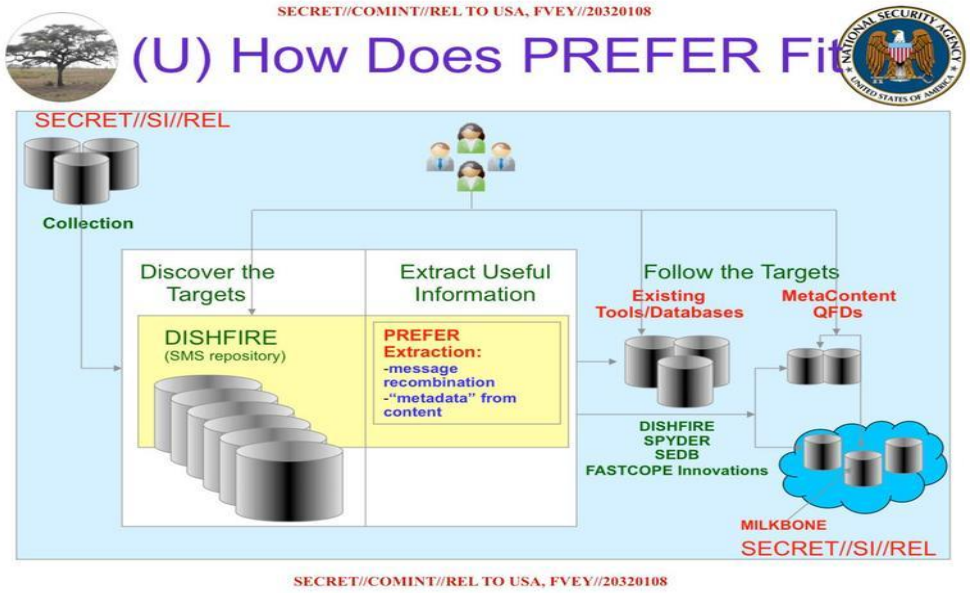
- **ECHELON,** originally a secret government code name, is a surveillance program (signals intelligence / SIGINT collection and analysis network) operated on behalf of the five signatory nations to the UKUSA Security Agreement[1]—Australia, Canada, New Zealand, the United Kingdom and theUnited States, also known as the *Five Eyes*.

- A radome at RAF Menwith Hill, a site with satellite uplink capabilities believed to be used by ECHELON

Carnivore, Dishfire

- **Carnivore,** later renamed **DCS1000,** was a system implemented by theFederal Bureau of Investigation that was designed to monitor email and electronic communications. It used a customizable packet sniffer that can monitor all of a target user's Internet traffic.

- **Dishfire** (stylised **DISHFIRE**) is a covert global surveillance collection system and database run by the United States of America's National Security Agency(NSA) and the United Kingdom's Government Communications Headquarters(GCHQ) that collects hundreds of millions of text messages on a daily basis from around the world.



Agencies

- Five Eyes
- BND
- DGSE
- FSB
- MSS

Five Eyes

- ## Five Eyes

The **Five Eyes**, often abbreviated as **FVEY. An** intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are bound by the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.

Bundesnachrichtendienst German

BND Agency

- **Bundesnachrichtendienst** (German pronunciation: [ˌbʊndəsˈnaːχʁɪçtnˌdiːnst], **BND**; CIA code name *CASCOPE*[2]) is the foreign intelligence agency of Germany, directly subordinated to the Chancellor's Office. Its headquarters are in Pullach near Munich, and Berlin (planned to be centralised in Berlin by 2016, with about 4,000 people).

General Directorate for External Security

- The **General Directorate for External Security** (French: *Direction générale de la sécurité extérieure*, **DGSE**) is France's external intelligence agency. The French equivalent to the United Kingdom's MI6 and the United States' CIA, the DGSE operates under the direction of the French Ministry of Defence and works alongside its domestic counterpart.

Federal Security Service of the Russian

- The **Federal Security Service of the Russian Federation** (**FSB**; Russian: is the principal security agency of Russia and the main successor agency to the USSR's Committee of State Security(KGB).

Ministry of State Security (MSS

- The **Ministry of State Security** (**MSS**) is the intelligence agency and security agency of the People's Republic of China (non military area of interests), responsible for counter-intelligence, foreign intelligence and political security. It is headquartered near the Ministry of Public Security of the People's Republic of China in Beijing.

Part IV -

- REFROMS FOR Pakistan's National Security

Pakistan's National Security

Reforms for Pakistan's National Security

- Selection criteria for Recruitment in Armed Forces and Law enforcement agencies should be reviewed .
- Induction of Foreign Qualified Professors in Civilian Units of Armed Forces and law enforcement agencies.
- Grade 6-12 Students' curriculum should include chapters about homeland security, Defense, Histories of various countries, success and defeat stories of Armed Forces ,Histories of Wars
- Conflict Resolution Problems should be included in College Students' Curriculum to resolve an international or national conflict or issues of war during exam.

Reforms for Pakistan's National Security

- Languages of other countries
- Languages of Pakistani areas
- Cultural studies of various countries
- Cultural studies of various nations in Pakistan
- History of foreign countries
- Science and Technology Education
- Vocational Education
- Liberal Education

Reforms for Pakistan's National Security

- Trainings should be arranged at Schools and College level for Bomb Disposal ,Fire Dept, Human Safety trainings ,Disaster Management trainings during Flood, Storm , Terrorism, Accidents ,Bomb Blast ,Preparedness Trainings for Domestic or International Attack.

- War and Peace Time Trainings for Preparedness for any Emergency Situation.

- Special Language Education to learn Indian , Afghani ,Russian, Chinese, Iranian ,Arabic, English , Israeli, English ,Spanish, French and other European and African Languages , should be provided

- Induction of Anthropologists, experts and University professors from International Relations, Strategic Studies, Criminology , Cyber Security , Engineering ,Computer Science , Economics ,Statistics and other related disciplines in Country's THINK TANK for National Security .

Reforms for Pakistan's National Security

- THINK TANK Members from Academia and Scholars from Research Organizations and Schools of Professional Studies should be consulted before a plan for war to understand the consequences of War in terms of its effects specially on Country's Economy, Infrastructure, Society ,humans and on the entire nation in general
- Beside inducting Diplomats after passing the Competition Exam from Federal/Provincial Public Service Commission the induction of Foreign and National Qualified Professors and PhD Faculty in the areas of International Relations, Foreign Policy, Strategic and Defense Studies is very essential.
- People should be educated to eliminate or reduce local and regional conflicts.
- Education and training for International Lobbying is very important for graduates in International Relations and Strategic and Defense Studies.

Technology for Pakistan's National Security

Investing in technology

- Achieving operational advantage over potential adversaries depends on investment in technology. The current impact and widespread influence of technology in our world stems directly from increased consumer demand and better manufacturing techniques. It is also the product of earlier scientific research, which in turn depended on investment, whether by the public or private sectors.

- The global availability of technology combined with an ever-increasing pace of technological change means that, in delivering the country's defense and security, we face an increasingly capable and diverse range of threats. These are likely to include not only sophisticated military weapons, but also greater innovative and ingenious application of readily available civil technologies. Where adversaries can more easily buy high technology products on the open market, this potentially reduces our operational advantages

- To understand, counter, and protect against such threats, we need to be able to use effective investment in defence and security science & technology to access and deliver technology into our future systems and equipment to provide operational advantage.

- Given the critical role that science & technology plays in supporting our immediate needs and programmes, we will need to manage carefully the balance between this and addressing our future capability needs. We also need to ensure our own technical capability, infrastructure, and research organisations are carefully prioritised to retain our ability to be an intelligent customer, develop specific solutions, and maintain credibility with our allies.

- Whilst we need to adapt and use more civil technologies to meet our defence and security needs, there remain areas of technology development where the market is weak, including Chemical and Biological Defence (CBD) and countermeasures for counter-terrorism (for example, electronic surveillance). These will continue to require focused investment in science & technology beyond what is provided by civil commercial markets

- We are, therefore, carefully prioritising investment in science & technology. It is our intention to sustain this investment at a minimum of certain percentage of the defense budget.

Being an Intelligent Customer of Defense Technology

- Almost all technology development derived from current global science & technology investment is driven by the consumer market. We need to draw on and leverage this investment, but to succeed we need to know what to buy, where it can be bought from, and where we need to focus our own investment in science & technology.
- We need access to the knowledge and expertise to integrate civil technologies into our defence and security systems and equipment.
- We need to understand the inherent strengths, opportunities, and weaknesses in how it is used – in particular, when the protection of individuals is at stake.
- Equally vital is the provision of effective and accurate advice on defence-related and security-related science & technology in times of crisis or emergency; this is particularly important in being able to adapt rapidly to new security situations and respond quickly to urgent operational requirements.
- The role of an intelligent customer for science & technology – its acquisition, use, and application – is therefore critical to our success in defence and security activities.

- Success as an intelligent customer nevertheless presents its own challenges. As well as knowledge of a particular technology - how we plan to use it operationally and how it was designed to be used through-life (including subsequent upgrades and insertion of new technologies)
- We must understand and assess the market place, what is potentially available, who the suppliers are, and what processes and standards are being used.
- This can be achieved through greater sharing of defence and security problems, thereby helping suppliers provide the most viable solutions from the market, but it also requires further investment in the tools, techniques, and expertise to assess market products and services.

- An intelligent customer has to be able to apply systems-level thinking and to understand how to integrate commercial off-the-shelf products, designed for markets with a high degree of certainty, into evolving defence and security systems and equipment.
- We have, therefore, to be able to identify, understand, and evaluate the technical, financial, interoperability, and security risks involved in such integration.

- Improving our understanding of commercial products needed to address these challenges will require investment. The understanding needed will be different at various stages of the acquisition process, including in-service and disposal; such understanding will also vary according to the complexity of our requirements and systems.
- The Government is not able to sustain deep technical expertise in all areas of science & technology: access to trusted sources of information and retained experts with a broad knowledge regarding use of technology, rather than deep knowledge in a particular area of science & technology, will be required.
- Once potential solutions have been identified, demonstration within a realistic environment will be needed to provide effective comparison and to understand the integration issues.
- Being an intelligent customer is also vital where we choose to procure or assess bespoke systems. In general, the Government retains responsibility for safety and operational risk, so we will need to maintain sufficient in-house expertise to understand those risks properly.

- In addressing the challenge facing us as an intelligent customer for science & technology in defence and security, we should prioritize investment towards providing timely and effective advice to Ministers and decision-makers.
- This includes maintaining a lean, skilled workforce in-house. We will also shape our expertise and access to expertise in developing and assessing markets and keeping up to date with the latest developments; and we will develop tools and techniques to assess, integrate, and evaluate our equipment and systems requirements

Investment of defence-related and security-related science & technology

We should focus investment of defence-related and security-related science & technology over the current Comprehensive Spending Review period in order to achieve the following six critical outcomes:

1. support current defence and security operations; enabling technology solutions to be developed to address urgent and current operational issues
2. plan for future capabilities that will be needed in the longer term; researching new science & technology particularly aimed at developing and fulfilling the capability generations that follow those currently in use or in procurement, ensuring the needs of Future Force 2020 and beyond are addressed

3.Cost reduction and more future proof systems; using science & technology to provide solutions and challenge approaches to defence and security capability, to ensure the long-term costs of such capability are reduced, thus ensuring approaches to our defence and security capability are adaptable to future requirements and technology evolutions

4- Support to critical science & technology capabilities/facilities; ensuring critical infrastructure, skills, and facilities are maintained to enable intelligent customers status in critical areas and sovereignty in key technological areas

5- Provide timely and effective advice to Ministers and Government; ensuring scientific and technologically based evidence and analysis is available to support Ministers and Government in decision-making, policymaking, and reviewing defence and security capability

6- Particular focus on the human and sociological aspects of capability. providing scientific and technologically based solutions to training, coaching, ethos, leadership, health of our Armed Forces and security personnel, as well as understanding influence, human sciences, and psychological approaches in military and security operations

Seeking the best and most advanced civilian technology

- It is critical that large companies make best use of their supply chains, including SMEs (Small & Medium Enterprises) and academia, and in particular follow an open systems design approach, to ensure that best technology in each domain is offered to Government.
- It is also important that industry and academia collaborate to facilitate this. We should promote such collaboration by greater sharing of information on our defence and security capability requirement.

CONCLUSION
Technology Awareness & Exploitation for National Security

- In order to achieve best value, we must access the results of the much wider and more extensive civil investment in research and development for use in Country's defence and security.
- This will drive down costs, influence other markets' investment, and expose new technology solutions to defence and security requirements.
- Access is available through both tracking technology development and engagement with the greater range of suppliers active in the wider civil markets for technology.
- These suppliers are vital to helping the Government achieve this goal and we must improve the communication of our needs and of our willingness to invest in these innovators.

CONCLUSION

We recognise in particular that:

- • Governments are the leading customers of defence and security goods and therefore our procurement approach and the differing approaches in other countries shape the defence and security market; and
- we have an economic policy objective to achieve strong, sustainable, and balanced growth that is more evenly distributed across the country and between industries.

Pakistan's National Anthem- by American Students

Thanks

Special Thanks to:

- NSA USA
- TSO UK
- ISPR Pakistan

- Audience