BARRISTER HARUN UR RASHID

Historic US strategic military shift

ON January 5, 2012, President Barack Obama proposed a historic shift in the US military's size and ambitions, scaling back its ability to wage the type of war and occupation that just ended in Iraq as the administration seeks to cut defence spending over the next decade. Under the proposal the following is proposed:

- The Army would face a 14% reduction in troops leaving it with too few to conduct two grueling ground wars at once, long a strategic imperative of the Defence Department;
- Reductions in the nation's nuclear arsenal; and
- A delay in the Pentagon's most expensive weapons, such as the F-35 stealth jet made by Lockheed Martin Corp.

Defence officials said the Army, currently at 570,000, likely will shrink to about 490,000.

A strategy document released said the military will be redesigned to fight one war using air, land and sea forces, while still being able to take on involvements in another region.

Overall, the plan envisions shrinking military spending by $487 billion over 10 years, a cut of about 8% in coming years, according to Pentagon figures. While the president has wide latitude to set military priorities, specific cuts the Pentagon will announce in coming weeks, must be approved by Congress.

President Obama said the nation was "turning the page" on a decade of war. But the president and Pentagon leaders said they weren't abandoning the US role as the preeminent global power.

"Our military will be leaner, but the world must know the United States is going to maintain our military superiority with armed forces that are agile, flexible and ready for the full range of contingencies and threats," the president said in a rare appearance by at the Pentagon.

Obama said he wouldn't repeat the mistakes of past administrations by crippling the military through post-war cuts. But some Pentagon officials -- anxious to stave off the possibility of further reductions -- said the proposed reductions will be as deep as those after Vietnam and the Cold War when cuts in annual emergency war spending are counted.

The strategy document reflects the Obama administration's preference for operations such as the war in Libya, which entailed a large coalition of nations and no US ground forces. The strategy also touts the utility of US special operations forces, which have decimated the leadership of al-Qaeda.

Also emphasised in the new strategy are counterterrorism operations -- missions using special operations forces that create only a small overseas footprint and work with local forces. Intelligence and surveillance will take on increasingly important roles, meaning the Air Force fleet of unmanned drones is likely to grow.

A new US emphasis on Asia is reinforced by the strategy as the Pentagon plans to shift its focus and resources away from Europe. The Pentagon sees challenges in China's military modernisation and is planning the new military approach to more aggressively counter Beijing's "anti-access" technologies, weapons such as China's DF-21D anti-ship ballistic missile, used for keeping US ships at greater distances.

Defence Secretary Leon Panetta said the military still will be able to respond to multiple crises at once, deterring aggression around the globe. "Make no mistake, we will have the capability to confront and defeat more than one adversary at a time," he said.

But, he said, "The Army and Marine Corps will no longer be sized to support the large-scale, long-term stability operations that dominated military priorities…over the past decade."

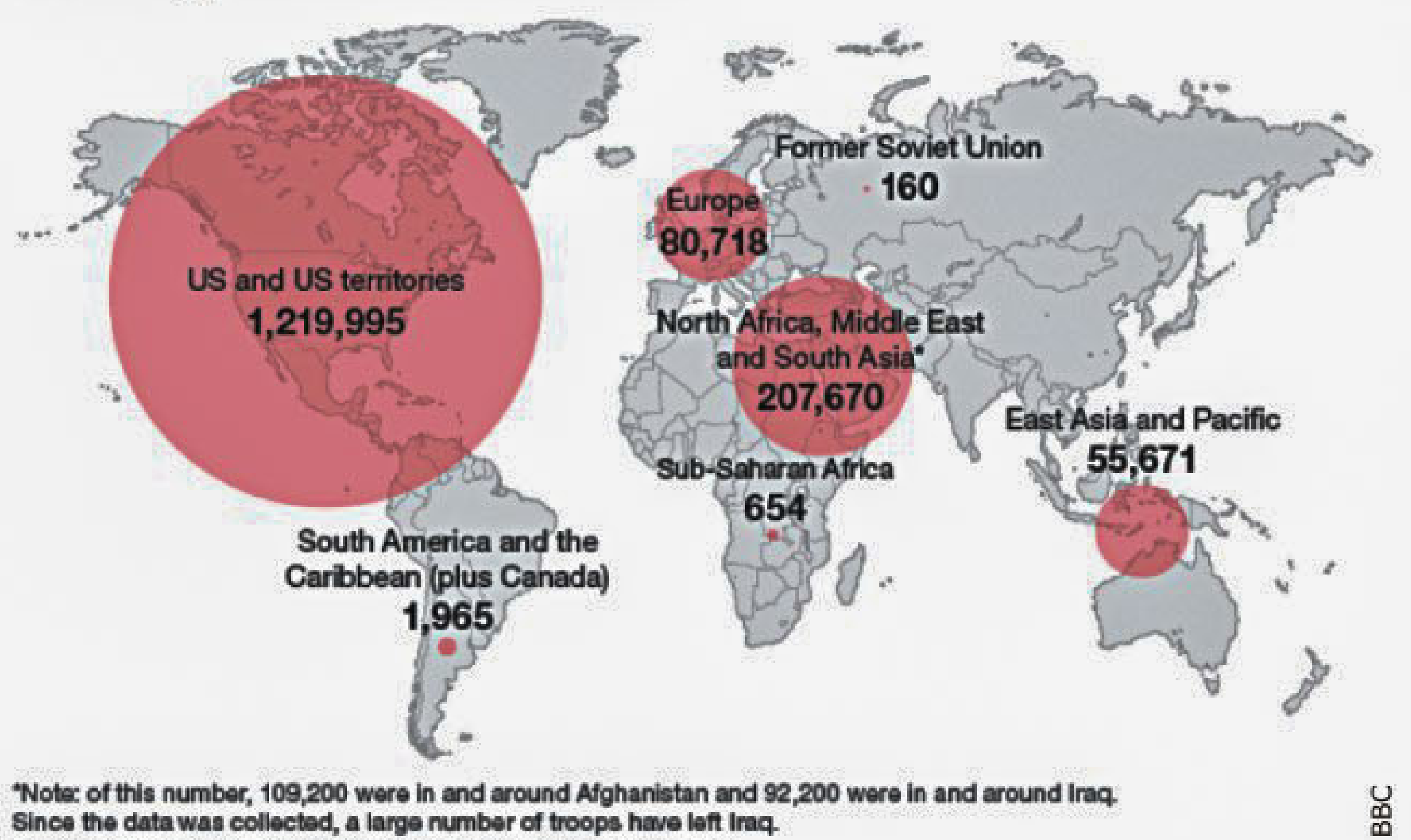
Panetta and defence contractors have argued for months that the planned cuts, while tolerable, are quite steep. But they have contended that an additional $500 billion to $600 billion in cuts over the next 10 years triggered by last year's congressional deal on the country's debt ceiling would be ruinous for the military.

Panetta said "The capability, readiness and agility of the force will not be sustained if Congress fails to do its duty and the military is forced to accept far deeper cuts. That would force us to shed missions and commitments and capabilities that we believe are necessary to protect core US national security interests. And it would result in what we think would be a demoralised and hollow force."

Obama approved a buildup of forces in Afghanistan, but administration officials have always viewed counterinsurgency operations with skepticism. The new strategy reflects the administration's view that counterinsurgency conflicts are too costly, while yielding murky results and incremental gains for international security.

Defence officials said they wouldn't abandon the military's expertise in conducting stability operations, but would move some of the resources to military reserves. That would preserve the ability of the Army to conduct limited counterinsurgency.

US military personnel around the world



*Note: of this number, 109,200 were in and around Afghanistan and 92,200 were in and around Iraq. Since the data was collected, a large number of troops have left Iraq.
Source: US Defense Manpower Data Center, figs as of Sept 2011

BBC

Reaction within the US

Announcement of the strategy prompted a swift response from Republicans. Sen John McCain said the US couldn't afford a "budget-driven defence strategy" but said he would review the document released by the administration. "I understand the need for reductions in defence spending, but we must also address the broader cultural problem plaguing our defence establishment: the waste, inefficiency, and ineffective programmes," Sen. McCain said.

Retired Army Lt. Gen. David Barno of the Center for a New American Security, a centrist think-tank that is often aligned with the administration, said the plan "fails to address the elephant in the room: whether this strategy can hold up under the weight of further defence cuts," particularly additional cuts contained in the debt-ceiling agreement Congress reached last year.

But Charles Knight, co-director of the Project on Defense Alternatives, which advocates more aggressive defence-spending cuts, said the administration's plans were "only baby steps" towards greater fiscal restraint.

Criticism is likely to grow in coming weeks as details of the cuts emerge. Key Republican presidential candidates, including Mitt Romney and Rick Santorum, have proposed increases in defence spending, and have criticised proposed Pentagon cutbacks in the past.

China's initial response

China in its first reaction to the US policy shift, the *Global Times*, owned by the People's Daily, a Communist newspaper, said that China would "pay the price" if it retreated in order to appease the United States. Further it said, "of course we want to prevent a new Cold War with the US, but at the same we must avoid giving up China's security presence in the neighbourhood region." China's Foreign Ministry did not respond as of writing this paper.

IISS View

The defence spending as a percentage of GDP in 2009 by London-based International Institute of Strategic Studies (IISS) was as follows: the US-4.7%, Russia-3.1%, UK- 2.7%, France- 2.1%, China-1.5% and Germany 1.4%.

Turning to 2011 edition of *The Military Balance*, published by IISS which is as ever comprehensively global in its scope, one key theme stands out that Western states' defence budgets are under pressure and their military procurement is constrained.

But in other regions, notably Asia and the Middle East, military spending and arms acquisitions are booming. There is persuasive evidence that a global redistribution of military power is under way.

In an atmosphere of economic stagnation, Western states' defence budgets are declining. While making significant cuts to Britain's defence capability including its ability to contribute to future expeditionary operations beyond Europe, the announcement by Britain and France in November last that they were 'opening a new chapter' in their bilateral defence cooperation that will include creating a joint expeditionary task force, and collaboration on aircraft carriers.

Finally, it is already clear that as a result of shifts in the global distribution of economic power and consequently the resources available for military spending, the big powers including the US are engaged in shifting their priorities in key areas such as quick deployment of troops including stealth aircraft and unmanned systems to address a crisis situation.

The writer is a former Bangladesh Ambassador to the UN, Geneva.

MIRZA SADAQAT HUDA

Cyber-terrorism: Truth or hyperbole?

THE debate on cyber-terrorism ranges from predictions of an 'Electronic Pearl Harbor,' where chaos and destruction resulting from cyber-terrorism attacks on critical infrastructure and communication systems would result in riots, panic and death, to the dismissal of any genuine threat and attributing the media and government as contributors to the hyperbole. To derive a pragmatic opinion on the contemporary threat posed by cyber-terrorism, a non-partisan analysis of definitions, perceptions and facts must be undertaken.

Cyber-terrorism is an opaque concept and its ambiguity is attributable as much to a lack of consensus on definitions, as to conflicting perceptions on the severity of the threat. John Blane has defined cyber-terrorism as 'premeditated, politically motivated attacks by sub-national groups, clandestine agents or individuals against information, computer systems, computer programs and data that result in violence against non-combatants and targets.' This definition gives rise to several deficiencies when applied to real-life scenarios. Terrorists make use of the internet to communicate with each other, recruit members, raise funds, organise activities and distribute propaganda. Since these activities do not constitute violence as a direct consequence, there is ambiguity as to whether they should be included in the definition of cyber-terrorism. In 1999 David Copeland downloaded terrorist handbooks from the internet to build bombs which killed 3 people in London. The terrorist attacks in Mumbai in 2008 were significant not only due to the unprecedented carnage that followed but also due to the use of satellite imagery and internet phones to plan, communicate and coordinate the attacks.

Thus even if the use of computers and the internet does not directly cause violence, it can be an auxiliary to terror attacks and an effective tool for furthering the terrorist's political agenda. Cyber-terrorism as a broader definition is 'the convergence of cyberspace and terrorism which enhances the terrorist's ability to communicate, plan and inflict terror through a network of operatives and cells and is closely entwined to non-virtual terrorist activities and global terrorism.' It is also important to note that cyber-terrorism is distinct from information warfare as cyber-terrorism is about causing fear and harm to anyone in the community, while information warfare has a defined target. For the purpose of this article, a confined definition of cyber terrorism, as it directly relates to causing loss of life, fear and violence through attacks on computers and information systems and which bears a political or ideological motivation, will be used.

AFP

The debate on cyber-terrorism is centered on two conflicting schools of thought. Advocates of the cyber-terrorism theory argue that it can be a preferred method of terrorist's modus operandi, as it provides a range of relatively anonymous, non-lethal options (for the terrorist) that can be applied at the speed of light with relatively low risk of escalation. The likelihood of getting caught, let alone incur military operations by the affected country is low compared to the possible benefits. As terrorists have a limited amount of funds, cyber-attacks are more tempting as they require less people and less resources. Richard Clarke, a terrorism and cyber-security analyst has stated that cyber-security is a serious threat to critical infrastructure in the US. From a national security viewpoint, a determined and talented cyber-terrorist could hack into a utility or chemical plants' SCADA (Supervisory Control and Data Acquisition Systems) and cause an accident to kill not only the plant workers but thousands of people in the surrounding areas. In the US, 300 critical infrastructure facilities lie in densely populated regions with 50,000 or more local residents. Scenarios similar to the Bhopal disaster are envisioned in the aftermath of such a cyber-attack. Of particular concern is the vulnerability and openness of the network systems operated by these critical infrastructure facilities. Dr. Harvey Kushner, an expert on terrorism believes that free flowing structures of modern terrorist cells would be highly effective in undertaking freelance cyber-terrorism against Western infrastructures which would be ideologically supported by rogue nations.

Experts who downplay the threat of cyber-terrorism argue that despite the hype surrounding it and the billions of dollars invested by governments and corporations to protect against cyber-attacks, the fact remains that as of date, there has been no fatality related to a cyber-attack. The National Counterterrorism Centre of the US in its annual report accounted for 13,186 deaths due to terrorist attacks in 2010, majority of which were a result of conventional methods of terrorism, including suicide bombings, armed attacks and kidnappings. Not a single attack was attributed to cyber-terrorism. This massive discrepancy between the casualties of the two mediums of terrorism is enough to compel the casual observer of the audacity of spending time and money on cyber-terrorism defence, when the real threat emanates from conventional means of terrorism. Despite no precedence to the 'Electronic Pearl Harbour' idea, governments continue to warn and legislate around the issue. Gartner analyst Richard Mogull has stated that although terrorists continue to use the cyber infrastructure to support their activities, terrorist use of the internet to deliver a significant digital attack is impractical and unrealistic. This is substantiated by security expert Bruce Schneier who stated that the hype of cyber-terrorism is inflated by the United States government and terrorists are more likely to attack via conventional methods.

One of the greatest fears projected by cyber-terrorism is external manipulation of SCADA systems used in critical infrastructure facilities. This theory, when analysed further, appears to be rather primitive and simplistic. Many analysts state that SCADA systems are more robust and resilient than cyber-terrorism theorists would have us believe and are likely to recover from a cyber-attack quickly. Power blackouts, water disruption, air traffic disruptions and other scenarios resembling cyber-terrorism often occurs without being a threat to national security. Cyber-terrorists would thus have to attacks multiple targets for extended periods of time to create terror and have any significant effect on national security.

Thus it can be concluded that cyber-terrorism is not as prevalent a threat as many in the defence and IT field would have us believe, but the underlying causes for terrorist's reluctance to use this medium must be evaluated:

1.Systems are complex and it may be harder to control a cyber-attack and achieve a desired level of damage than using conventional methods. Unless people are injured, there is also less media attention. Tried and true methods and operational success will take precedence over sophistication of attacks. Damages incurred by cyber-attacks can be fixed quickly via system re-instalments and back-up files whereas damages to physical infrastructure including complex machinery and expensive facilities through conventional means of attacks would incur more time and recourses to fix; and

2.If a critical disruption or malfunction occurs due to a cyber-attack, in the case of absence of any physical damage to infrastructure, the operators of the attacked site may deny that the disruption was due to a cyber-attack. This would defeat the purpose of terrorism to instil fear and attract global attention to their cause.

Thus it can be concluded from the above analysis that cyber-terrorism as compared to conventional methods of terrorism at present time, poses a minimal amount of threat. Although cyber-crime and information warfare do pose threats to individuals, businesses and states, cyber-terrorism, in its definitional form, is not a serious threat and has been over-estimated by governments and over-hyped by print and electronic media. This does not denote that cyber-terrorism will not pose a significant national security threat in the future. The future will see deepening economic dependency on computers and this poses greater risks of losses due to disruptions which can adversely affect aviation, communication and financial services. The growing complexity and interconnectedness of these computer systems means that a disruption in one may lead to disruptions in others. Cyber-terrorism could also become more attractive as the real world and cyber world become more connected, with a greater number of physical devices attached to the internet.

In the present time however, since the damages from conventional terrorist operations are of greater magnitude as far as spreading fear and causing fatalities are concerned, national security should be focused on preventing such traditional means of asymmetrical warfare. In the words of Dorothy Denning, 'For now, the truck bomb poses a much greater threat than the logic bomb.'

The writer is a Research Associate, BEI.