



USAF personnel oversee electronic warfare mission data flight testing

## **Letter from America**

By Gp Capt Carl Scott

We depend on our allies in the United States to deliver the influence we, as a Service, as a Nation, currently achieve on the global stage. Their arguments are, largely, our arguments; their perceptions, perhaps too frequently, foreshadow our own. It is my hope in this series of articles, to offer an insight, personal and flawed as it may be, into the debates which are shaping thinking in the United States. An occasional letter from America. In this first note, written in the summer of 2008, two key areas have dominated thinking in the United States: The contribution of the Air Force to current operations, and the balance between the capability required to meet that challenge and that of future wars, the second, related issue, was the implication of Russia moving forces into Georgia. A reminder that states will still play on the global stage, seizing advantage of perceived weakness or distraction.

#### **Air power & counterinsurgency (COIN)**

*'...any major weapons program, in order to remain viable, will have to show some utility and relevance to the kind of irregular campaigns that, as I mentioned, are most likely to engage America's military in the coming decades ... the perennial procurement cycle – going back many decades – of adding layer upon layer of cost and complexity onto fewer and fewer platforms that take longer and longer to build must come to an end.'*

Secretary of Defense Robert M. Gates, May 13, 2008 (Remarks to the Heritage Foundation, Colorado Springs)

*'...Our troops are taking a hammering. The current operational environment, counter-insurgency, irregular warfare against non-state actors, 'war amongst the people', is*

*likely to prevail for the next twenty years. This is the infantry war. We should change the basis against which we resource and train, from large-scale interstate conflict to peace-enforcement, with a consequent change in balance of resource between the land, air and maritime environments. We need high calibre, well motivated and led soldiers, who can serve as social workers, medics and policemen, building infrastructure and intelligence networks, training the host nation, and we need a great many more of them. Our troops are taking casualties, too many casualties. They need protected mobility. They need counter IED capability, as an absolute priority. Resources need to be directed to meet their needs, not legacy cold war projects with no relevance in the current operating environment. We need to change with the challenge of the times. It is our moral responsibility in Defence to deliver a responsive, adaptable capability, or more soldiers will be lost, unnecessarily...'*

How very true.

But if you want the troops to take a greater hammering, if you want to lose more bodies: withdraw airpower. Take the resource out of space and cyberspace.

Counter-intuitive as it may seem at first glance to the armchair warriors, it is space, cyber space, and air that is delivering success, that is allowing a small number of highly trained personnel to have a disproportionate effect on the battlefield, that is preventing the mass of deployed forces from becoming targets, hostages in their own sprawling encampments. It is these domains of warfare that deliver situational awareness, power projection, reliable communication nets, secure mobility, logistic resupply, and timely, accurate targeting. The persistence,

agility and precision that is required to deliver in the current operational environment is the gift of air and its associated domains. The soldier cannot achieve the persistence and precision, the flexible scale of force or the agility required to contend with the challenge of global networked, intelligent and informed opponents, without air.

Flooding the battlespace with more personnel, more infanteers, more logistics and staff officers, even if we could recruit, train and retain the great number of highly educated and fit individuals required, would only serve to increase the perception of invasion and occupation on the part of the host nation and his cultural allies. It would also increase the targets available to our opponents and our own exposure to the frailty and equivocation of our own media and politicians.

There is a debate raging in the capital of our greatest ally. Should resource be channelled into maintaining a strategic capability advantage over future opponents, exploring emergent technologies, fifth generation fighters and directed energy weapons, and the emergent domains, space and cyberspace, or should we focus on fighting the current war, on victory in Iraq and Afghanistan?

This is no mere intellectual exercise, heads have been taken. The Chief of Staff of the Air Force, and the Secretary for the Air Force, his civilian counterpart, have both been removed from post. Apparently as a consequence of failures in nuclear weapon handling, they would argue this was a consequence of their support for future programmes, holding the line on a strategic vision for the USAF,



**General Norton A Schwartz, Chief of Staff, US Air Force**

accepting the need to address today's conflict, but not at a price of losing the edge when the next major challenger arises. Defense Secretary Gates is drawing on his own experience in the Central Intelligence Agency to shape a new balance, driving through change in an Army that appeared to have wilfully curtailed its capacity to engage in COIN operations following the debacle of Vietnam<sup>1</sup>. He is seeking to ensure the relevance of the enormous investment, in blood and treasure, by the people of the United States. He is seeking to maintain the deterrent effect of its recourse to force, and avoid another embarrassing defeat for the global power.

His strategy appears to be working. General Petraeus has developed an effective formula for the conduct of COIN operations, the surge of troops into Iraq has reduced the levels of violence in target areas. It is a triumph for the Army and for Secretary Gates. The United States Air Force has become mired in controversies over funds spent on 'comfort capsules' for senior officers to travel in luxury to war zones, over the Byzantine procurement processes for large fleets of replacement aircraft,

over sponsorship for their display team, the Thunderbirds. Deprived of its Commander, the USAF is obliged to wait for the Senate to endorse a replacement, months with caretaking, not strategy, at the helm while the new Commander rises to the challenge of transforming the organisation.

In the straitened times that face our own military capability, these arguments are relevant. We may not choose to place heads on sharpened stakes in the media in the American manner, though with the increasing tendency of our Senior leaders to engage in fratricidal media operations, this may not be long in coming. We do, however, compete for limited resources, we do establish policies that gather momentum, or inertia, and become a legacy for our successors and all too often, a constraint on our front line. We do engage in narrow, tribal thinking to reinforce our own position and weaken our competitors. There is nothing new in this. It is natural that organisations act in their own interest. But it would be unwise to confuse that self-perpetuation for reasoned argument about the needs of the battlefield. Human lives depend on clarity and rational thought.

It is worth examining the reality of conflict, and the surge period in Iraq in particular, before taking a look at future challenges, both within and without the current paradigm for irregular warfare.

The Petraeus doctrine is expressed in US Army Field Manual 3-24, which looks to accentuate the 'soft power' aspects of military presence to win hearts and minds. It seeks to steer the pragmatic and reductionist tendency in US military thinking away from 'kill and capture' and the discredited metric of the body

count, toward a more meaningful engagement with a population, empowering the host nation to act, through the medium of intelligent, well trained soldiers mentoring and supporting indigenous forces.

In 2007, in order to implement this approach, 30,000 US soldiers were extended or surged into operations in Iraq. Violent incidents fell significantly by the end of the year. The doctrine was, apparently, effective.

However, polling<sup>2</sup> in Iraq suggests the effect was not one of 'winning hearts and minds'. Some 63% of the population felt the surge had had either no effect or a negative effect. 79 % had no confidence in American troops and 42% believed attacks on US Forces to be justified, suggesting either the doctrine had not been implemented as intended, or the outcomes were not as predicted. The impact on the global stage is less easy to determine, but the perception of US occupation of an Islamic population continue unabated and Al Quaida has continued to recruit on the strength of the operation.

Nor, it seems, was there a significant reduction in 'kill and capture'. Early indications<sup>3</sup> suggest Iraqi deaths were 25 – 50% above the preceding year. Those accused of insurgency and held in US managed prisons also rose from 15,000 in 2006 to 25,000 in 2007<sup>4</sup>. Few, if any, of the surged troops were the highly trained counter-insurgency forces capable of integrating into the host nation and guiding its efforts. These were the same troops held over, deployed early or called up from the Guard units of the small towns of America. Dedicated, committed to the task and ready to take up arms in the

cause of Democracy, but no different from the many who had preceded them.

### **So why did hostile activity decline in 2007?**

Detaining 25,000 potential insurgents would undoubtedly have an impact in the short term (though how it might affect the long term is less clear). The arming and 'legitimation' of warlords in tribal sunni and shia areas, largely segregated as a result of years of kidnap, torture and forced migration, would reduce some of the freedom of manoeuvre for insurgents, particularly those recruited abroad. The third element, which surged alongside troops on the ground, was the deployment of airpower. Kinetic airstrikes were acknowledged by Congressional Research Service<sup>5</sup> as a major factor: 'one of the major shifts has been in the kinetic use of air power.' But airpower has been historically condemned in the COIN environment for lack of discrimination, for the counter-productive effects of collateral damage, for its lack of persistence and the inability to act in a timely manner against transient targets.

### **Historically**

And therein lies the significant change, self-evident to anyone who has sat in an operations room in Afghanistan or Iraq, who has watched the change in balance between air and land over persistence and precision. A soldier cannot remain amongst a hostile populace for protracted periods, building an understanding of pattern of life, assessing movements of key individuals, understanding their habits and associations. Air can, and does<sup>6</sup>. The very presence of a military unit, heavily protected and moving to retain tactical surprise, changes that which is observed. Silent and invisible, air



**A USAF F-16 releasing a Paveway III laser-guided bomb**

does not. The collateral effect of the soldier, his presence, the munitions he deploys, is significant. The precision of air munitions has increased to the point that its accuracy, both in determining and destroying the right target, is far beyond that achievable by ground based systems, armour or indirect fire. From the inventory of complex sensors and non lethal munitions, through the low speed, intimate support afforded air manoeuvre forces by helicopters and UAVs with hellfire to the panoply of low yield, high precision bombs, there is an arsenal of precise, controlled effect sitting over the battlespace with the ability to respond to a spectrum of triggers. As one combatant told the New York Times<sup>7</sup>: 'We pray to Allah that we have American soldiers to kill...these bombs from the sky we cannot fight.' Air power inflicts on the insurgent the kind of psychological effect that he seeks, through improvised explosive devices and ambush, to have on our own people. Increasing troop numbers on the ground increases vulnerability to hostile action, offering ever greater footprint, support personnel and targets, increasing the psychological and media effects achievable by the insurgent. Fewer, better soldiers, with the right

training and resources and recourse to persistent and effective air, space and cyber capability make a significant difference. It is proven on the ground in Iraq and Afghanistan by SOF every day.

The competition between states, between nations and peoples, between cultures and identity blocks is a constant throughout human history. When one power dominates the globe with a strategic advantage that no conventional opponent can match, the opposition, those whose interests diverge, or who do not associate themselves with that power, naturally seek to exercise influence on global events through alternate strategies. Unconventional warfare is the current paradigm. Network enabled, media aware virtual organisations can wreak havoc on a militarily dominant, but technologically dependent and democratically open society, as a parasite may on a far more complex organism. The ability of the current Islamist threat to evolve and respond to changes in our behaviour is remarkable. Intelligent and highly educated minds are engaged in identifying and targeting vulnerabilities, modifying approaches as we, in turn, evolve to meet the challenge. Understanding and defeating this opponent lies initially in the cyber domain, with the necessary vigilance to prevent attack and prosecute arrests enabled by the associated air-space-cyber domains. But this does not make a conventional strategic advantage redundant. As soon as that advantage is lost, the competition will return to the historical norm; rivalry expressed through political, diplomatic and military conflict. The United States dominates the global stage, both militarily and culturally. The vitality of its economy, the capacity for innovation

and intellectual inquiry is, for the meantime, unparalleled. Unparalleled, but not unchallenged. China and Russia have legitimate interests, as does an emergent Europe, India and Iran in ensuring their influence over their neighbours and the global economy. The role of the state is to ensure the security and interests of its Sovereign entity are met. The global system is not an amiable village populated by liberal idealists, it is a turbulent pool of sharks. As soon as a strategic advantage is lost, it is challenged. That is why we are not speaking latin. Dominance creates power balancing behaviours and the United States is creating a great many. China and Russia have the intellectual and technological resource to probe weaknesses in emergent domains. They continue to develop approaches to warfare which will, if the situation affords, become the basis for open competition. Thus the vision of the United States Air Force in acknowledging the need to lead in space and cyberspace and resource the conventional strategic advantage is wise and deserves applause. However, the challenge is to meet the requirements of the current operation whilst resourcing preparations for the next, with finite resources and strengthening opposition, internal and external.

That is a challenge which necessarily translates to our own sphere, our own interest, in the United Kingdom. We cannot afford to underestimate the contribution of air in the current conflict, or our dependency on it, and its associated realms of space and cyberspace, in the next. The speech by Secretary Gates, frequently used in Washington to query procurement programmes for Air and Maritime environments, stands further examination:



*'There is a good deal of debate and discussion – within the military, the Congress, and elsewhere – about whether we are putting too much emphasis on current demands – in particular, Iraq. And whether this emphasis is creating too much risk in other areas, such as: preparing for potential future conflicts; being able to handle a contingency elsewhere in the world; and over-stressing the ground forces, in particular the Army. Much of what we are talking about is a matter of balancing risk: today's demands versus tomorrow's contingencies; irregular and asymmetric threats versus conventional threats. As the world's remaining superpower, we have to be able to dissuade, deter, and, if necessary, respond to challenges across the spectrum.'*

The test of any putative capability should indeed be relevance to current operations and what we can predict of future conflicts. It must, however, be acknowledged that our predictions of future conflicts and strategic events have been consistently inaccurate. Thus, our best safeguard is flexible capability, systems that can adapt, with geographical and operational reach, yet capable of operating with intimacy. Our capability must not be contingent on the interests of our defence manufacturers, or the internecine struggles that distort the historical record and pervert departmental policy. We must acknowledge, with clarity and impartiality, what it is that delivers the necessary effect now and has the adaptability and growth potential to meet the uncertain demands of the future. Global reach and ubiquity have long been essential elements of air, but as technology accelerates, airpower is entering an era of unparalleled adaptability, persistence and precision. It is at



**Su-25 Frogfoot ground attack aircraft**

the very heart of our success.

#### **Russian tanks and cyber war**

As Washington basked in its customary summer torpor and the world's attention was turned to the Olympic gathering in Peking, it might have seemed, if only for a moment, that the old truths were behind us. We live in a new world, with new challenges. China, India and Brazil rapidly ascend the developmental ladder, soaking up global resources; a gradual, relentless deterioration of the environment pressures populations and borders, small groups of radical muslims crouch in caves and dream of caliphates, soldiers must become armed social workers and airmen, eyes in the sky.

Then with an alarming jolt, the old ways intruded into the reverie.

Columns of Russian armour, self propelled guns and mounted infantry, pour through narrow defiles in the Caucasus. Ground attack aircraft, spewing out infra red decoy flares, arch over unseen huddles of vulnerable people. The familiar craters of heavy

munitions fill the screen. Refugees amass, diplomacy falters, the media rails against brutality and injustice.

It all seems so anachronistic. The same Russian soldier had straddled his gun-turret entering Kabul, and Prague, and, seemingly, Berlin before that. So where were the massed ranks of soldier-social workers and cross-governmental strategy groups and streamlining tiger-teams? Is there room for discourse when armour grinds its way through fields of fire? When the guns roar, surely only overwhelming force can win the day?

Of course not. Military force can resolve nothing. Those armoured columns can break a great many things, destroy lives, infrastructure and people, but they can resolve nothing. They are an eruption of the many frustrations that arise from ill-defined borders, conflicting identities and sparse resources. It takes diplomacy, negotiation, recognition of cause and effect, rational analysis and open dialogue to resolve the complex issues that fuel aggression. Morality and just cause are rarely self-evident. Shades of grey abound in the world where solutions are crafted.

**So what is there to learn from this event?**

If we were to follow the example of Hezbollah, and there are worse coaches in this turbulent world, we would respond by rebuilding infrastructure, opening financial opportunities, improving quality of life, providing medical and social care to victims of this dispute. We would attract the wavering masses, not assume the right to punitive action. Lest we forget: The Soviet Union was brought down by Coca-cola and Marlborough, not Pershing and Minuteman. Lebanon was won by

provision of social services and medical care, not by Israeli bombardment.

So, what may be drawn from this unfortunate venture in the Caucasus? Behind the screen of grinding armour, a new line of development, trialled and debated elsewhere, was brought into focus. Flawed, as yet in its infancy, but coordinated and brought to bear alongside the traditional martial activities.

As the border fell behind the advancing troops, the computer systems of Georgia were assaulted by an overwhelming wave of hostile activity, a wave oblivious to physical borders and nationalities. Web sites and communication systems used by the President, Parliament, Ministries of Defence and Foreign Affairs and the media in Georgia were disabled. It was an imperfect assault, as it did not disarm the air defence system, which continued to harass the ground attack aircraft pummelling the infrastructure and deployed forces of Georgia. Nor was it able to seize the archaic infrastructure of the target country, which was, in all probability, protected by a veil of obsolescent technology. But it was, for the first time, a coordinated arm of a major attack. Previous cyber operations have been conducted by the Russians in concert with diplomatic pressure. When the Government of Estonia decided to move a memorial to the soldiers of the Great Patriotic War, built by occupying Russian Forces in their capital city, the country suffered 24 days of disruption which closed the banking system and forced major changes in approaches to maintaining infrastructure and social cohesion in the absence of computer networks. The leading suspect behind the attacks, in Estonia and Georgia, is



an organisation known as the Russian Business Network, though it would be exceedingly difficult to prove any link to that organisation or to the Russian government. In this domain the aggressor can enjoy the anonymity of the internet, as a virtual non-state actor, while furthering national interest.

Don Jackson, director of threat intelligence for SecureWorks, an Atlanta computer-security company, analyzed the Internet traffic during the attacks and found evidence of outsiders breaking into and erasing data from Georgian government servers. He traced the attacks from what he called a 'cyberinfantry' to servers used both by the Russian Business Network and the Russian government...Russian embassy spokesman Yevgeniy Khorishko denied any Russian government involvement. 'Russia is not responsible for that,' he said. 'How do the Georgians know that these are Russians? We have nothing to do with these attacks.' He said Monday Georgia has blocked access to all Russian Web sites – ones that end in the suffix ru...It is difficult to determine who is behind a cyberattack. Georgian government officials tapped into an international network of cybersleuths in countries such as Germany, Estonia and the U.S. They moved government information to servers in Germany and established backup systems in Estonia, which has become an international expert in cyber-response since its government Web sites came under attack last year, by what is believed to have been a Russian adversary.<sup>8</sup>

The anonymity and ease of access, low cost and low risk for the technologically literate, raises a new dilemma for state control of the instruments of

power. An individual, pressure group or niche interest could conceivably initiate, escalate or sustain diplomatic pressure, and potentially armed conflict, beyond the control of the sovereign state, which begs the question: Which is more worrying: Russia choosing to use a deniable capability to conduct operations against bordering states, or Russia having no control over extremist groups who launch attacks to meet their own interpretation of national interest? What value has diplomacy in resolving conflict when the State has no control over combatants? How do you seek to deter or coerce an anonymous assailant, who may be a nation state, a criminal or an adolescent prankster?

*'Cyberattacks are now a staple of conflict -- whether authorized or unauthorized,' said Paul Kurtz, a former aide to the U.S. government's National Security Council. Such attacks are particularly unpredictable because they can be launched by groups outside of the government, which can escalate crises even as governments are seeking to diffuse them, he said.<sup>9</sup>*

Russia is not alone in developing this kind of capability<sup>10</sup>. They are simply the first to expose their own use of the cyber domain in armed conflict. Others may have exploited the cyber domain. It has been alleged, for example, that in 2007 Israel closed down the Syrian Air Defence system in order to attack selected targets with impunity<sup>11</sup>. If such an attack did take place, then it achieved its objective, it was discreet, effective and deniable. The Syrians can only wonder whether their own system or operators underperformed, or whether Israeli tactics were beyond their detection capabilities. If this was the case, if this attack took place under the shroud of cyber warfare, then it would expose

a peculiar vulnerability of air forces. Technologically highly developed, networked and utterly dependent on complex computer systems, they are absolutely vulnerable to this kind of attack. None of this is lost on potential opponents, who seek asymmetric approaches to counter the overwhelming superiority of American and allied forces. China, where cyber warfare is an acknowledged element of Defence doctrine, stands accused of launching thousands of probing forays a month into U.S. computer systems, military and civil, for commercial and military advantage. Chinese intrusion has been noted in the IT systems in US Secretary of State for Defense's office, the Pentagon, Chancellor Merkel of Germany's office and, it is suspected, the top 300 British Corporations. A particularly ingenious ploy allegedly involved incorporating a 'Trojan horse' into an electronic picture frame, sold widely through the USA, which responded to computer connection by introducing a programme that disabled antivirus programmes and passed any passwords in the system to the manufacturer in China. Naturally, the Chinese Government denies any involvement.

Whatever the source of these attacks, whoever is probing and developing capability, the necessary response is the same:

*'Cyberspace has become integral to the joint fight...We expect all of the services, to include the Air Force, to provide personnel who are trained and who know how to operate systems in cyberspace...they must know how to be able to defend cyberspace, how to be able to support-intelligence operations in cyberspace, and if we're directed, to be able to do offensive operations in cyberspace.'*<sup>12</sup>

It is not a uniquely 'Air Force' problem. The collapse of the financial system, power generation and distribution and communications are a challenge to us all. The loss of industrial, commercial and financial information has repercussions throughout society. But, within the sphere of military operations, the increasing dependency on complex communications and data systems is most evident in Air Power, and thus the burden falls to Airmen to develop responses and seek to insulate our core capability from the damage which can be so readily inflicted at so little cost to the enemy.

*'... the formation of Air Force Cyber Command was a stroke of genius by the Air Force secretary and chief of staff to focus Air Force resources and efforts on this problem, quite frankly, because we're so dependent on it...Our value is in the cross-domain integration of air, space and cyberspace, to create combined effects on the battlefield for the production of sovereign options . . . that there may be misperceptions that the Air Force's purpose is to 'protect the nation, or protect the Department of Defense'. But all of the services have organizations that do, in some ways, what we do. The creation of the new command is about the Air Force focusing resources, energy, direction, money and programs, for the protection of command and control capabilities so that Air Force elements are available for the joint fight.'*<sup>13</sup>

It is not too late to develop the capability to counter this challenge in the United Kingdom: but we are entering the race late, and we may not be recruiting the correct demographic to display the creativity and technical innovation required to match the resources already invested by our potential opponents. We may, like the cavalryman who could not envision a role for the aircraft over

the battlefield, or the Naval officer who denied aircraft could influence maritime warfare, be incapable of comprehending the ultimate scale of the challenge posed by this peculiar dependency, and the impact of assault. But we can begin generating the momentum required to ensure our next generation of airmen are masters of the domain. Armour may still cross borders, air forces may choose to destroy infrastructure and deployed forces, but they will do so with impunity, in an entirely different context, if our own mechanisms of state are disabled, along with the ability to command and control our forces, to bring force to bear in our own defence. We ought, at least, to thank our Russian neighbours for this timely reminder of the realities of the shifting nature of power, and our own developing weaknesses.

#### Afternote

There may be solace at least for the advocate of manned aircraft. Once you take the man out of the cockpit, you may create considerably more complex, and vulnerable, dependencies than you can defend.

The author is deeply indebted to Charles J Dunlap Jr, for his article *Making Revolutionary Change: Airpower in COIN Today* available at <http://www.carlisle.army.mil/usawc/Parameters/08summer/dunlap.pdf>

The speeches of Defense Secretary Robert M Gates can be found at <http://www.defenselink.mil/speeches/secdef.aspx>

#### Notes

1 For an engaging perspective on the US Army in the post-Vietnam era, see Richard A Clarke 'Your Government Failed You'. Ecco New York 2008.

2 ABC News/BBC/ARD/NHK Poll, "Iraq Five Years Later: Where Things Stand," 17 March 2008.

<http://www.abcnews.go.com/images/PollingUnit/1060a1IraqWhereThingsStand>.

3 Jim Michaels, "19,000 Insurgents Killed in Iraq Since '03," USA Today, 26 September 2008,

[http://www.usatoday.com/news/world/iraq/2007-09-26-insurgents\\_N.htm](http://www.usatoday.com/news/world/iraq/2007-09-26-insurgents_N.htm).

4 Gordon Lubold, "Do U.S. Prisons in Iraq Breed Insurgents?" The Christian Science Monitor, 20 December 2007.

<http://www.csmonitor.com/2007/1220/p01s01-woiq.html>.

5 Catherine Marie Dale, Operation Iraqi Freedom: Strategies, Approaches, Results, and Issues for Congress Washington: Library of Congress, Congressional Research Service, 22 February 2008.

<http://www.fas.org/sgp/crs/natsec/RL34387.pdf>.

6 'The Air Force recently watched one man in Iraq for more than five weeks, carefully recording his habits—where he lives, works, and worships, and whom he meets . . . The military may decide to have such a man arrested, or to do nothing at all. Or, at any moment, they could decide to blow him to smithereens.'

Mark Benjamin, "Killing 'Bubba' from the Skies," Salon.com, 15 February 2008, [http://www.salon.com/news/feature/2008/02/15/air\\_war/](http://www.salon.com/news/feature/2008/02/15/air_war/).

7 Barry Bearak, "A Nation Challenged: Death on the Ground," The New York Times, 13 October 2001.

8 Wall Street Journal, August 12, 2008, 'Georgia States Computers Hit By Cyberattack'. Siobhan Gorman.

9 Ibid.

10 'The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. In 2005, the PLA began to incorporate offensive CNO into its exercises, primarily in first strikes against enemy networks.'

Annual Report to Congress: Military Power of the People's Republic of China 2007. OSD. [www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf](http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf)

11 'Why Syria's Air Defences Failed to Detect the Israelis.' David Fulghum, Aviation Week, 03 Oct 2007.

12 Gen. Kevin P. Chilton. Commander U.S. Strategic Command, July 17 2008, address at Maxwell AFB, Ala. <http://www.af.mil/news/story.asp?id=123108010>.

13 Maj. Gen. William T. Lord. Commander of Air Force Cyber Command, Barksdale AFB, La, July 24 2008, address at Maxwell AFB, Ala. Ibid.

## **This article has been republished online with Open Access.**

Ministry of Defence © Crown Copyright 2023. The full printed text of this article is licensed under the Open Government Licence v3.0. To view this licence, visit <https://www.nationalarchives.gov.uk/doc/open-government-licence/>. Where we have identified any third-party copyright information or otherwise reserved rights, you will need to obtain permission from the copyright holders concerned. For all other imagery and graphics in this article, or for any other enquires regarding this publication, please contact: Director of Defence Studies (RAF), Cormorant Building (Room 119), Shrivenham, Swindon, Wiltshire SN6 8LA.

 **ROYAL  
AIR FORCE**  
**Centre for Air and  
Space Power Studies**

**OGL**