**King's College London**
**Liddell Hart Centre for Military Archives**

## Annual Liddell Hart Centre for Military Archives Lecture

### Information in Conflict: Who Really Commands the High Ground?

**by Nik Gowing**

**given Thursday, 2 March 2000**

---



---

## Introduction

It is only fair to say that when Lawrie Freedman called me last summer and asked me to deliver this lecture tonight I was somewhat surprised. I could not suppress my John McEnroe instincts; 'You cannot be serious,' I suggested. After all I am merely part of an enormous broadcast machine reporting the day-to-day, real-time developments in a proliferation of conflicts. Given the distinction of Liddell Hart's work, and his contribution to the understanding of conflict, I wondered if Lawrie was taking one helluva risk. An hour and a half from now, you will be able to pass your own judgement. But as I reflected in recent months, I revisited Lawrie's own paper on the changing forms of military conflict to the IISS 40th annual conference in Oxford eighteen months ago. With a flattering tribute to my own 1998 study of the failures in information handling in the African Great Lakes crisis of late 1996/early 1997, he flagged explicitly both the shortcomings, and the misguided nature of western assumptions of information superiority in modern conflict. What I want to do tonight is throw forward that work in a considerable leap, based on work I have been doing for some time. I speak in a personal capacity. I will use examples – which is why all the gizmos are here. And I ask for your forbearance if there is any momentary snarl up. I will dig much deeper into Lawrie's original theme.

## Information in Conflict: Who Really Commands the High Ground?

Information in conflict – in other words war and the whole spectrum of emergencies - who *really* commands the High Ground? And let me make clear – none of this applies to the domestic conflicts of Whitehall or national politics! I mean war, operations short of war, peace support, peace enforcement and so on. The general mindset in official government and military circles remains: 'We do. We have the systems so we will command the high ground without challenge, and almost as of right'. There will be some of you here who still believe and assume that. In the spirit of Liddell Hart, I will challenge that and present evidence.

I saw this billboard on the wall of the Liddell Hart archive here as I was researching an aspect or two for tonight. This *Daily Telegraph* poster is from his time as defence correspondent in the early 30's. It says, 'Best Military Information: Frequent articles'. It was a bold claim. In the un-real time then of telegraph communications, and cosy relationships with the brass, it was so easy to provide 'best information'. Indeed it was hard to challenge or question if it was anything short of best. How different in today's real-time world. I will argue tonight that whoever has the technology and processing skills to seize the information High Ground quickest in conflict, is likely to have greatest immediate impact, but well short of the best and most accurate information. Indeed as NATO discovered during the Kosovo conflict, what is assumed to be 'best' can often be found out as far from best.

Liddell Hart reports in October 1922, in *Elements of War*, of the commander's absolute need for prompt information, and reports rendered instantly. The principle is no different today. But how different 'instantly' is now to what it was then. And therein lie the many new problems and contradictions I want to highlight. No longer in this near transparent world of conflict information is it necessary to do what Liddell Hart reported both the Duke of Wellington doing well, and having to rely on - guessing 'what was at the other side of the hill'. As I will explain, web sites, satellite phone systems and the new robohacks will see to that. My analysis will make some of you feel uncomfortable. Some may disagree with me. A voice or two will demand: where is morality and ethics in the new undermining of a government's political and military assumption of commanding the information high ground? But however uncomfortable you may feel about this, morality really has no place in the new information dynamic. This new dynamic is driven mercilessly by the new technology. If it is not taken seriously it is likely to have a fundamental impact on the very credibility of any mission.

There are many contradictions but I put it to you there is a clear trend: Kosovo, Chechnya, India-Pakistan, East Timor. Much of what takes place can now be very visible to all of us – if we chose. Based on Kosovo, my friend Michael Ignatieff is just putting forward the idea of 'virtual war'. The phrase is catchy, but I *do* wonder if the 'virtual' is not misleading. In many ways, from Sri Lanka to Sierra Leone, it could be re-labelled 'actual' war. So much so that we rather take for granted the greater real-time information transparency in conflicts like these. After breaking news in a TV bulletin, we can update on radio. Then for more facts, analysis and previous detail we can click immediately onto an on-line news site of our choice, to a deadline and time frame of our choice. Streamed audio and video can be called up whenever you chose. Soon there will be even more real time availability as bandwidth expands exponentially. In so many ways there is a supermarket of video and information - a proliferation of real-time information from theatres of complex emergencies and war.

Through an ever-expanding spectrum of delivery systems, notably satellites, we have more information coming in text, video and sound from more parts of the world than ever before. It is being delivered in real time, or as near as damn it. It is the age of *now*. Not two hours, two days or two weeks hence – but now. By the minute or by the hour - and from wherever you are - you can select which crisis you want to dip into or get an update on, and you can select from the proliferation of video or text outlets providing it. Which is why in my Harvard study I labelled this whole field the *tyranny* of real time – because real time can be so tyrannical, so cruel and arbitrary. Or, of course, you can protest overload and choose to ignore the whole damn lot. Much of what I have to say is not rocket science. Frankly, it is pretty damn obvious. But what I find time and again is how even those, like many of you, who know well the technology and the dynamic have not really joined up the dots. Often the implications

have not been worked through, especially for the making of policy, and especially when it comes to political and military engagement in an emergency, often short of war.

In principle – there are clear and specific implications for time, speed, accuracy, credibility and integrity. But whatever part of the real-time information world you might work in, it is becoming virtually impossible to find an acceptable equilibrium of these vital but conflicting factors. Additionally, overload and stress are a significant factor in who controls information now - or does not. These five factors lead to two further pivotal questions; how right are we getting the facts and who is getting it right? Despite the buzz of the new technology, the answers are not what most people expect.

Seymour Hersh's recent extended analysis in the New Yorker (6 December 1999) of how overload is creating the US Intelligence and National Security Gap certainly confirms many observations and conversations of my own. How, despite the inevitable official claim that all is well, official systems in of all places the National Security Agency at Fort Mead are overwhelmed by the sheer volume of data transmitted by e-mail, fibre optics and also encryption. Yet it is the NSA which is charged with handling and unbundling this information. Hersh quoted a former CIA Director of Operations as concluding, 'The dirty little secret is that fibre optics and encryption are kicking Fort Meade in the nuts'. But what I want to suggest to you, is that the new nature of information in emergencies is kicking everyone in the nuts. This includes those who think they are rather good at handling it because after all that is what they are in the business of. This can be in Fort Meade, government and military information-gathering machines of the most sensitive kind - or in every newsroom. Here in the UK, one senior military officer described the lack of robustness on handling real time information as a state of professional 'constipation'. In this new world of information proliferation, those who believe they hold ultimate power to influence and control it no longer do. They are challenged. More fundamentally, new technology is producing cheap ways under the traditional wire of official control of information. The traditional systems and assumptions can no longer cope or endure. NATO's experience during Kosovo provides a long predicted, but salutary lesson. It was compounded by all the problems of multi-nationality *and* different national views of information handling. Let me give you one example of explicitly how the new transparent information environment can so easily undermine – out of the blue. It does so in a way that leaves those with assumed information control realising how little control they really do have, even though they believe with all their massively expensive systems, they *should* and *must* have that control.

## The role of Robohack

[Video clip of individual broadcasting from the Albanian border]
What would you do faced with this? Here is a screw up by (your own) NATO forces all recorded in a transparent battlefield. Where is the control here? This is inside Albania in June 1999 on the Kosovo border, with NATO aircraft overhead on a mission to attack Kosovo. This was not the product of news organisations working to embarrass NATO. This was transparency created by the new reality of low-cost, lightweight technology that readily facilitates such access. The new breathtaking miniaturisation and capacity of information technology is making conflict, along with its inherent horrors and abuses, more visible and more transparent, and therefore more troubling for those who have chosen to engage in it.

I am talking here of the new challenge to politicians, the military, the warlords (what the ICRC call the New Warriors) and the humanitarian organisations. Rather than info-

dominance by the institutions of government in particular, I argue there is the opposite; there is convergence and overlap. What do I mean by that? Because of the new real time capability the information pillars are merging. There are no longer sharp lines of demarcation between the NGOs, media, government, diplomats, ministers and the military when it comes to information in conflict, and out of this, comes an ultimate but fundamental new paradox, an inverse relationship. Those warriors from democratic states who have the most sophisticated information gathering and processing systems in conflict, and are answerable to their Parliaments or alliance committees are, I suggest to you, the most constrained and troubled in their ability to make best use of it. Or more specifically, because of a certain callowness and lack of self-assurance in coping with this new real-time information challenge, they currently *feel* themselves more constrained. This in turn limits the willingness to take risks and engage with the kind of overwhelming and decisive military action needed to achieve an end state. Witness NATO in Kosovo, or the international community in the former Yugoslavia. In contrast, those thugs and new warriors with cruder, more basic and least sophisticated systems, who do not have parliamentary accountability breathing down their necks, who do not have such sophisticated information systems, and who have a ruthless determination to pursue war for revenge or taking territory, have a much greater capacity to intimidate, control information, control a conflict and thereby shut down what is known of the horrors they are perpetrating.

As the UN Secretary General concluded in his report 'Towards a Culture of Prevention' published in September last year,

> 'Even the most repressive leaders watch to see what they can get away with; how far they can tear the fabric of human conscience before triggering an outraged external response'.

An assumption of the power to control information is central to that. Chechnya in October to December 1999 was an example, until some brave journalists refused to be cowed by Russian intimidation and threats of the most dreadful revenge. Witness also Rwanda, and the Congo. The new information power of those equipped with the lowest level of sophistication is what I concluded in my study of the African Great Lakes crisis in 1996/7. The conclusion has been further sharpened since then. A significant percentage of Africa is currently at war, labelled Africa's first world war, with nine nations engaged in the Democratic Republic of Congo, and a separate battle for power in Angola, where any UN peace presence has been brutally rejected, most viciously in the shooting down of two UN planes by UNITA. But in all cases, outside international eyes have been firmly kept out. But my argument is that even in the world's nastiest, most inaccessible conflicts the number who will be able to hide what they are doing will become ever smaller.

Witness, for example, Sierra Leone and the bravery of one Sierra Leonian man, Sorious Samura, who bought himself a modest camera, and after dreadful experiences happened to meet the BBC's Fergal Keane in a Freetown chicken bar in January a year ago. That resulted in these horrific images being seen for the first time by the outside world, confirmation of the horrors being perpetrated *by all sides*. Let me make the central point vividly. The challenge to official assumptions of information control is from Robohack. [This cartoon interpretation is from the British National Union of Journalists four years ago, warning of the threat of work and technology overload in the foreseeable future.] Sorious Samura was a robohack. So was the amateur camera owner who shot the rough footage of the Kaduna riots in Nigeria at the start of the BBC 9 o'clock news last night; the camera bore witness however raw the quality.

Robohack does not make diplomats, genocidal warlords, the military or the humanitarians comfortable but his/her role is central to understanding the shift in the information centre of gravity in battlefield and peace operations. Instant telephone or satellite transmitter. Instant Video. Instant laptop. All uploadable by some form of satellite or radio uplink. Lightweight. Low costs. Highly mobile. Go anywhere. Transmit anything.

This is one type of Robohack at work during the anti-WTO Seattle demonstrations last December [picture]. The small camera, the knapsack, operating in the thick of it. Most importantly, this is maybe a few thousand dollars worth of equipment, no more. It produces high quality material, indistinguishable from the most professional. Think of its impact then, and watching the local TV station in Seattle last week confirms the impact of its output almost three months later – the evidence of police brutality. 'Shoot as much gas as you want in there now,' says a police captain, 'I want you to drench them'. (*Seattle Times*, 24/2/00). But, robohacks like this do not work for a traditional news or information-gathering organisation. They take a personal risk to gather real-time information for a medium of their choice where they believe they can earn the most money and/or make maximum impact and trouble or just record the events.

This article in the London *Times* about animal rights activists filming sheep exports at Dover docks (on the English south coast) underlines the new principle. The target audience no longer has to be the traditional outlet of radio, TV or newspapers that are instinctively assumed by those in power. In this fragmenting information market, there are now many other ways to exert influence and challenge traditional information power in a conflict. Remember - a conflict or emergency does not just mean war. It can be environmental, or human rights, or corporate abuse, or an oil tanker disaster. These ways are much broader than the news at 6.30 or 9, or the following day's newspaper. No longer are they just national; via the continuous news channels like BBC World or websites they are global.

Take Chechnya recently. For the first two months of the Russian Chechen conflict starting in October 1999, the Russian government successfully used its usual brutish and thuggish techniques to shut down the war zone to outside media ears and eyes. Look what happened to Andrei Babitsky of Radio Liberty. They intimidated possible robohack media travellers to Chechnya with videos and stories of the most appalling atrocities meted out to journalists and foreigners; images of hands and limbs severed during torture. But eventually robohacks penetrated the ring of steel to grab images that confirmed Russian losses of equipment and soldiers that up to this point had been denied. The squalor endured by injured soldiers was finally there to be seen. Vladimir Goussinsky is the rich and powerful media mogul who runs the independent Russian media group Media Most. He told me during the Davos World Economic Forum (31 January 2000) that after his private NTV channel finally took the risk of filming then broadcasting such images the opinion polls against the Russian military operation rose swiftly from a few percentage points to 56%. Despite the intimidation and threats, the crude Russian military assumption of full information control was thus undermined eventually in a dramatic political fashion. Only the final seizure of Grozny in early February probably prevented a public opinion backlash. As I said, I am trying to join up the dots.

It may seem trite when discussing war but the way Australian rugby player Michael Foley rushed to his kit bag to grab his own video camera at the end of the Australian rugby victory last autumn reinforces the ubiquity of this equipment, and the ease of use at any time – anywhere. The new reality of information in conflict is that anyone - any of you - can be a

robohack with your modestly priced cheap laptops, digital cameras and mobile phones. In theory any of you can now challenge head-on the governmental assumption of information superiority. It is 'You have been framed' in war. In North America, one of the most successful cable channels is Real TV that relies exclusively on videos of incidents recorded by amateurs. We, you, anyone, can gather and transmit information, as near as damn it in real-time.

In Chechnya the battle for information has been as much between the Chechen and Russian websites. The Kavkhaz website is real-time information. Without corroboration, the credibility and factual accuracy must always be doubted. As Bridget Kendall wrote recently for the BBC's *From Our Own Correspondent,*

> 'I jot down the details: the Russian general they say they have captured alive; the night-time ambushes that allow Chechen snipers to recoup daytime losses; it could all be lies, of course. Much of it probably is. But how are we to know?'

But on information in conflict, this is about what one perceptive, very senior commander recently described to me as 'the race for space'; how information like this readily seizes the high ground in any information void if there is no credible and more official version forthcoming – which is often the case. We are talking about data being available liberally, and being fed into the real-time assessments of those who choose to use it; East Timor, the Karen of Burma, M19, Columbia. There is now a proliferation of examples.

Like (after robohack) the Cybermonk, Father Sava. [Film clip] He is a young Serb monk from the Decani monastery in northwest Kosovo. The Cybermonk is fluent in English and despite his monastic duties, is highly versatile in the business of computers and websites. Until the start of NATO operations in Kosovo last March, Father Sava was providing real-time information with his (Serb) perspective of unfolding confrontations between Serb forces and Kosovo Liberation Army fighters in the immediate vicinity of Decani. Father Sava is just one example of the new mediums providing real-time information from a theatre of conflict or humanitarian emergency.

And the next challenge will be this [captured image ready for transmission of Nik Gowing giving his lecture] the image grabbed electronically and beamed instantly by e-mail. Africa may have fewer phone lines than New York City but none of this will depend on hardwire. It will depend only on the much cheaper robohack technology with expanding bandwidth and may be transmitted from anywhere. This too can be legitimate information from war and it circumvents traditional 'media' organisations. Imagine a grabbed e-mail image from Grozny of – say – bodies in Russian uniforms. The images can seize the high ground of public impact. But are they real Russians, or others faking death in Russian uniforms? Who can tell? But what about the impact? It is important to repeat that respected news organisations will be cautious and questioning when they filter this raw data. But what role for respected news organisations in future? It could be argued that their influence is already being threatened with being diluted because of the impact of the new technology. If that is the case, who else must government institutions deal with? Because building fast are the further challenges to official assumptions of information hegemony. Iridium is already here. The chunky handsets uplink to 66 Low Earth Orbiting satellites. (It makes you wonder about brain cancer). Iridium may be protected by Chapter 11 bankruptcy, because sales have never matched the great technological leap but the principle is clear. Those 66 satellites create a worldwide communications jacket that envelops the world in terms of real-time information. As the advertising blurb says, 'The freedom to communicate from anywhere at anytime'. Iridium is

another robohack facilitating getting under the official wire when it comes to real time information. Imagine if your politicians and military commanders were to repeat now the secret preparations for the Hail Mary left hook against Iraq in the desert in February 1991. The massive build up and logistics tail 400 miles northwest across the desert towards the settlement of Aa-Aa could be reported in virtual real time from robohacks taking the risk of venturing into the sand dunes and reporting live on Iridium.

In September 1999 the East Timor resistance proved that principle. One of their leaders David Ximenes had an Iridium set on the hills overlooking a burning Dili. He reported to resistance offices worldwide, and what they passed to media organisations was assumed to be accurate. Why not? It was fresh. It was immediate. It came from the scene. But now it is wondered how exaggerated, how reliable, some of the so-called 'eye witness' reports of murders and mass killings really were at the time. UN 'Interfet' forces never found the police station said by the resistance to have blood splattered walls and bodies piled high to the ceiling. What of the claims of up to 20,000 women raped in Bosnia in 1992 to 1993. The ICRC say that subsequently they have evidence of only some 400 cases – horrific yes, but on nothing like the scale assumed initially.

For us in TV news it is going further and faster and even more instantaneously. This is TOKO [picture]. It allows us to transmit TV images on an INMARSAT B satellite telephone. We cannot yet do this in real time. But its information power and value in places like Congo, Afghanistan and many developing countries is immense. This does the work of a half million-dollar dish. In terms of real-time information, hitherto inaccessible and remote locations have become highly accessible, and not just for war. For example, before TOKO, it would have been many days before any of us saw video of the alleged genocide in the rain forest of Eastern Zaire in late 1996; or the take-over of Kabul by the Taleban; or the massive flood impact on 20 million people of the devastating cyclone in Orissa in Eastern India last October. Instead TOKO provided horrifying video images within a day, once the robohacks had managed to fly in. Extend this principle to other locations in conflict and I hope you can see my point; that only on increasingly rare occasions can it be assumed there could be closed war and emergencies, hermetically sealed and beyond public view. India and Pakistan discovered this for the first time during the Kargil crisis in Kashmir last year. You would not have thought this had you heard the senior military response to a lecture I gave in Delhi in August 1997. After I alerted the senior officers and political figures of the new information technology that would create a new transparency in future conflicts, there was a clear, and stubborn belief that; 'We will always control information from any operation involving Indian forces'. But that is not what happened in Kargil and Kashmir. The grainy quality of the image confirms the hurried use of TOKO by my BBC colleagues to transmit at least something. TOKO had been hidden to avoid detection. [Video clip of Kargil.]

I am not here as a 'tecky' to give you an engineering briefing. I am trying to highlight how those in the institutions of democratically accountable governments, who assume they have control, will probably no longer have it even when they believe they will, and should. Public scrutiny in real time and of minute details must now be expected in any theatre of conflict of the world, even the most inhospitable and rugged location, like Kargil and Kashmir. Virtually nowhere is beyond reach now. Take the Pakistan coup in mid-October 1999. When any military force seizes power, the first thing they do is take full control of the instruments of information. They seize the radio and TV station to stop unauthorised transmissions. That's what General Musharraf's forces did. On location that very act was photographed and recorded digitally. In the past such images and video would have had to await official

sanction for transmission a considerable time later, or be shipped and/or smuggled out of the country eventually. But the first e-mailed images of the security forces entering the TV station were being transmitted worldwide a short time after this happened. The *very* power that these forces were seeking to impose was thus undermined, virtually immediately, via a PC, e-mail and the Internet. [Video clip of Pakistan coup.] And then not long afterwards, by way of TOKO, came the video itself. (Which is why I remind you of the power of this little camera.).

I use the Pakistan coup to illustrate a principle. The events themselves were rather benign, and certainly not violent. Indeed the vast majority of Pakistanis welcomed the coup. The darker side of the principle I am putting to you came in East Timor at the end of August/start of September immediately after the overwhelming UN-organised vote for independence. It exemplified the sheer arrogance of those at the top of the Indonesian military who have long assumed they have ultimate, unchallenged power – especially to do whatever they want in what they have long assumed will be always be an information vacuum defined and controlled by them.

As the UNAMET documentation confirmed even beforehand, the Indonesian military had been arming and preparing the militias to embark on dreadful acts in the event of a pro-independence vote. Three weeks before the referendum UNAMET had issued a specific warning. 'Immediate and firm measures will be required to avert a humanitarian crisis, or a war, after the ballot'. But the subsequent transparency that the military failed to shut down then alerted the rest of the world to the horror. As the two recent UN and Indonesian human rights reports just published confirm - that transparency also helped to identify and finger not just those carrying out, but more importantly those ordering the most dreadful, bestial violence designed to go a long way to eliminating a good proportion of East Timor's population. Real-time information found out the Indonesian military. In the case of BBC World, my BBC News colleagues were there in real time, reporting live by satellite. Robohack video rolled raw and unseen into our news machines, with anchors like me being able to describe the scene as it unfolded before my eyes, here with a ten second delay (just in case there were horrors in the raw video - at one stage we saw a man hacked to death virtually live on camera). This, for example, from inside the UN compound in Dili.
[Video clip of UN compound. Refugees climbing over the fence.]
Essentially it was real time. There was no ambiguity there. The central issue is speed, availability, vividness and impact. Such brave use of robohack technology exposed the strategy of death and killing by the Indonesian-backed militia. It was not quite fast enough to force a halt to the most dreadful of revenge. But it was fast enough to highlight to the outside world what was happening. With images like those of the fate of refugees even in the sanctuary of the UN, the ICRC or Bishop Belo's compound you can see how quickly the official cant and instincts of deception in Jakarta were unmasked as lies. Two months later it went a long way to help force President Habibie from power. More importantly it challenged the military assumption led by General of unchallenged power.

## Information in War and Emergencies

So in all these conflicts there is now a mass of information swirling around in the information and cyber environments, however you chose to label them. But discriminating good from questionable, and maintaining editorial filters in the process has become a major challenge, where the battle may be being lost. In something close to real time, both the warriors with evil intent, and military alliances with questionable end states defined for them by politicians

can be exposed, with their political justification undermined. Which is why I pose not just the question who really commands the high ground? But also, are they any good at it? After all, over decades the leading powers, especially the US, have spent tens of billions of dollars developing and deploying sensing systems. Those systems are designed to enshrine ultimate command of the information high ground by governments, the politicians and the military – almost as an unchallenged right.

By systems I mean the airborne monitoring and snooping systems like EC 130, AWACS, J-Stars and U-2; the National Technical Means – the communications and spy satellites; the UAV's – the unmanned aerial vehicles that can snoop almost silently over the horizon – steered and monitored in real time to provide a birds eye view; SIG-INT – the signals intelligence; and HUMINT – the on-the-ground human intelligence provided by the brave ones working undercover, in disguise, or indigenous operatives who provide information. I give you an incomplete list of systems that some of you will know in intimate detail far better than me. In theory all these justify the instinctive governmental, military and diplomatic assumption that they (you) command this high ground; that they (you) have overwhelming superiority; that they (you) have almost as of right a hegemony in information that cannot and will not be challenged. There is no questioning the volume of filtered and unfiltered information being supplied by these systems. The massive challenge (and frustration), as some of you know from personal experience, is filtering the information at speed, and discriminating the useful from the rubbish especially in a multi-national system. That takes time and skill. Often it cannot be done in real-time. Which is why I say the lower-tech ways under the wire have such impact.

All of us in a conflict zone now flaunt our sat phones and cellnet phones like virility symbols; we upload and download from our laptops; we plug in and we plug up. For example, on a balcony in Pristina one Saturday night after KFOR went in last June we watched Serb houses go up in flames - a KFOR officer, a British officer, the British diplomat and a journalist. We all talked to our offices on mobile phones – lined up. Who had a monopoly of information there? In Northern Ireland the RUC officers have mobile phones to call their wives and colleagues in a crisis. They circumvent the normal information loops of command. Their wives urge caution. On board ships, officers and ratings are not 'cybermonks', but 'cyber matelots'. Some ships now even have their own, uncontrollable Internet cafes for private use. Even in times of emergency the crew have private, authorised access to PC's, the Internet and e-mail that cannot be halted. What of the sailor on a chat-line, or private e-mail reporting a rumour that a plane has not returned to the carrier or other 'rumours' that circulate on board a ship before being confirmed or refuted. Even with an Official Secrets Act, who has a monopoly of information then? In Israel, young conscripts in their barracks or observation posts have the mobile phones taken off them because they might reveal to Syrian forces or Hezbollah from where they are talking to their boy and girlfriends. Again, it is the technology that is driving this issue. And the new commercial availability of metre-minus satellite images is already blowing away another military assumption of superiority.

The traditional mantra in defence forces about the 'Military and the Media' – with a sub-text of control - is thus simply an irrelevant mindset. The issue is far broader. It is information and how everyone handles it, both in theatre and outside. But how many minds have really moved? I often ask military audiences: surely there cannot be any of you who genuinely believe what I heard one NATO 3 star say to me at a NATO exercise at AFCENT in Brunssum (Netherlands) in October 1998, literally a few months before NATO's Kosovo air operation. The three-star declared from his heart; 'The Media are the enemy'. 'Our aim,' he

added, 'must be to avoid, evade and mislead'. He then added, 'My plan in any operation would be to stick them in a cupboard and throw away the key'.

I don't recognise the planet he lives on, works on, and commands forces on. The media are now just one part of the information matrix in a theatre of conflict or peace operations or complex emergency. Do not think otherwise. As the Kosovo operation showed, spin may provide a certain political virility. But it cannot deny facts revealed by the new information technology. In military circles especially, the instinctive response can still be, 'Damn Meejah'. What the hell are journalists doing undermining our mission? And we are 'Reptiles', the label affectionately given us by UNPROFOR spokesman Gary Coward during the Bosnia conflict. Smart, flaky skin with the ability to snap unexpectedly. Such knee-jerk descriptions enunciate an understandable irritation. But they also betray an unwillingness to embrace the new real time realities that I am laying out for you. When I was in Pristina in Kosovo on 26 June 1999, two weeks after the KFOR insertion, where would that NATO three star (and he was not joking) have found a cupboard for the 3,842 media personnel accredited to be with NATO's KFOR forces at that time? It would have been an enormous cupboard! 3,842 meant one media person (including engineers) for every 5 KFOR personnel.

When it comes to war, conflict and humanitarian emergencies, more important is the question, what is media now anyway? The challenge and threat is from 'media' with its purest, widest and most accurate meaning; a proliferation of mediums – a medium being any channel of communication. Therefore media or mediums no longer means a well-known, well-established news organisation like the BBC, Canadian Broadcasting, Reuters, Associated Press etc etc. It means *any*one and *any* medium, whether e-mail addressee, website (wherever that originates from), or someone with the electronic capacity to record and transmit information, sometimes covertly. Or is it propaganda?

The images of the downed US F1-17 near Belgrade during the Kosovo war were readily dismissed on the NATO side as 'propaganda'. It was an inevitable, understandable knee-jerk reaction. I suggest this kind of near real-time information should never be labelled as propaganda. This stealth wreckage, including the pilot's name and serial numbers, was not manufactured at a Serb film studio and shipped in to deceive. The downing of the F1-17 was fact. Robohack images like this were undeniable confirmation, corroboration, of a loss, even though the US Airforce, fearing for its pilot in a ditch 200 metres away refused even to confirm the plane had disappeared.

Similarly, while inconvenient and ultimately embarrassing for NATO, the images of the mistaken bombing of the Djakovica refugee convoy provided hard evidence, not propaganda, of a tragic bombing error by NATO warplanes. Even if the cameraman was escorted by Serb officials, this was the tyrannical, the cruel and arbitrary power of robohack at work, albeit with a propaganda twist added by Belgrade in terms of claims of who did what, and what vehicles were on the road. We all witnessed Jamie Shea's predicament as the images seized the High Ground and the NATO military, for their own reasons, denied him hard information on what happened or might have happened. NATO was caught out. Not by what the mindset readily labelled as propaganda but by hard, undeniable evidence on video that something dreadful had taken place.

We have the same problem with the robohack video shot and made available by a Russian that emerged last week from Chechnya. Russian officials immediately labelled this as propaganda. Yet it confirmed in its horrific way how Chechens of fighting age have ended up

dead, with blatant displays of Russian contempt even towards the bodies. Who? How? We do not know for sure. But by its very existence, the video seizes the high ground with the clear impression that Russian forces have committed war crimes. And when it comes to commanding the information High Ground, the story is far from over.

This *Washington Post* cartoon showing the conflict between War and News crystallises the contradictions in the two questions I asked near the start: How right are we getting the facts? And who is getting it right? Whether military, media or whoever, we all want to command the information high ground with hard facts. But real-time technology is pushing us all closer to the need to provide a first version – which can often be similar to rumours without the most extensive fact checking. The trouble is that as the Allied Rapid reaction Corps concluded after its first months in Bosnia, 'First reports are inevitably wrong'. Yet it is those reports, the rumours that have the profound, unstoppable public impact. In this real time world it could be said there is a 'Race to be wrong' as all involved try to secure the information high ground with less-than-perfect information, whether humanitarians, the media, the military or anyone. The Pentagon official, who said this after the Kosovo conflict, was right in my view. But in this race to be wrong, or the race to take a view, is there also be a race to distort or exaggerate with impressions or rhetoric that stake out a high ground? What credibility in this new digital age? What capacity and ready temptation to distort?

[Doctored photo: Blair]
Firstly, look what can be done: how reality in this real-time world can be warped in an instant – in this case with a mouse or electronic keypad and wand.
[Doctored photo: Team]
Again this is not rocket science – but it highlights the potential for mischief when lives and national reputation is at stake. I am talking of impact by way of manipulation.
[Doctored photo: Royals]
And it is not confined to the 'Damn Meejah', or the untrustworthy press. This is the family photo of the British Royal family at the 1999 wedding of Edward and Sophie in Windsor Castle. Ten faces were deemed not happy enough. So, as *The Times* confirmed, those ten faces were altered digitally so that even the Queen and her grandson looked happier.

Where will this principle end in war, conflict and misrepresentation in a Real-Time battlefield? You will be familiar with the row at CBS TV in the US over their imposing electronically the CBS logo over a large NBC billboard on Times Square in New York City on Millennium night. Secondly, what about claims and rhetoric which seize the high ground? Claims which are uncheckable, possibly exaggerated but a politically convenient misrepresentation? Take the language. In the first days after the start of NATO's Kosovo air war on 24 March last year. As even senior officials now concede, from Day 3 of the Kosovo conflict British government ministers and other NATO colleagues began exaggerating claims of genocide against the people of Kosovo. It was an understandable emotional response by ministers, but genocide is a specific term describing the annihilation of a race. Such descriptions may have served the political purpose of securing the information high ground. But as even Human Rights organisations admitted, Kosovo was not a genocide, and never appeared that way despite the dreadful horrors taking place. I certainly asked myself, 'So what is the evidence they have?' Officials have said somewhat uncomfortably, 'It was an understandable worse case projection based on assumptions not hard facts'.

The principle can also be applied to the early claims of making 'substantial damage' to Milosevic's military machine. Such exaggerated claims secured the high ground but they

eventually returned to haunt the credibility of those politicians and senior military officers who chose to make them *without* incontrovertible corroboration. In the end the claims of genocide were never challenged because Milosevic's expulsion of 800,000 Albanians dominated public perceptions. But as I have heard at several recent conferences, knowingly using exaggerated rhetoric in this new real time world is a dangerous principle to adopt because the chances of being caught out are high indeed.

So where does that leave the dilemma in that struggle for the information high ground? Where do any of us position ourselves when it comes to upholding our credibility and integrity, without joining the race to be wrong, and being wrong in public? Let me graphicise crudely that dilemma starting from the moment of crisis: I suspect many of you will know from personal experience what I mean. It comes out of the blue leaving a series of physical, political, military, humanitarian or commercial bombshells that takes everyone by surprise.

[Video footage showing a sequence of reports on a developing crisis]
This is the crisis. If you like it is point zero, the point from which we then watch what happens over time, say a period of 36 hours. We watch what impact is created. (Notice I cannot calibrate impact – just give a sense of enormity). This is how generically I would define the response curve before the new tyranny of real-time emerged say five years ago. This is the information edge, the high ground, that participants in the crisis – media, government, military, warring factions etc. – might have been trying to secure. High, but still modest impact; time to maximum impact maybe 3-4 hours as the information was collected and transmitted using only modest. Less-mobile real-time capabilities. This struggle for the information edge was controllable. That was the past, the very recent past. Now let's look at where we are in the new real-time tyranny of the present and what lies ahead. A much sharper curve; bigger amplitude, much shorter wavelength. The new and growing proliferation of information shortens the impact cycle before other information or bombshells flow in from elsewhere, and other matters take over. To use the nuclear analogy – an increasingly short half-life. There is a vicious, virtually instantaneous impact over a very short period of maybe no more than an hour – in reality it can be minutes. Look where this generates the new information edge: higher, more instantaneous, far greater impact, a much more frenetic cycle, compared to where we were *before* the tyranny of real-time.

In this flawed real-time environment this is what we are all struggling to secure in crises and real-time emergencies. Those first minutes, maybe the first hour or two, but no longer. It is not about sitting on information or prevaricating. It is about reporting. It is about getting it right. It is about getting the information out as fast as possible. But how right do you get it if you move rapidly to secure the high ground on the information edge, and secure attention? The deaths of the two Gurkhas in the Kosovo explosion was luck. The British military enjoyed a delay of some five hours simply because no journalists were in the vicinity. Brigadier Sebastian Roberts would say the delay which allowed the news release to be managed was more luck than any judgement.

But generally, how much do you compromise your integrity? Rumours instead of news? This is the point of F3 – the dilemma of F3. First? Fast? But the price in real-time. How flawed? If you wait, will you be right, but will you have failed to secure the high ground on the Information Edge. This is the heart of the information challenge that faces us all. You have to decide. It is F3 that challenges our mutual capacity to handle real-time information at the speed dictated by new technology; a capacity that I suggest is deteriorating. As a very senior NATO officer told me a few weeks ago with exasperation; 'We have all the systems, but still

we do not have the human software to process the information. We have a major disconnect'. And in the Kosovo crisis we have discovered *just* that.

What kind of crisis incident am I talking about? Let me give you one powerful, vivid example that strikes right at the core. I am going to give details and take you through the scenario and the reality for the next 15 minutes. What would you have done? This is about transparency, robohack and the fact that all the information supremacy that a large military alliance *believes* it has, is not the same as the new reality of the robohack environment. Let's go back to 1 May this year, 1999, to that moment of bombshell and crisis. This flash report on the Agence France Press agency wire at 13.48. It was datelined; Luzane, Yugoslavia (AFP). It read, 'At least 23 passengers in a bus were killed in NATO air raid on a bridge in Kosovo on Saturday, an AFP reporter said'. In the BBC World newsroom we were cautious. AFP is not the agency with the best reputation for accuracy. I was due to go on air at 14.00, twelve minutes later, to present the hourly bulletin. The daily NATO briefing from Brussels was due to start at the same time, or just after. What do we do? My duty editor instructed us to hold off, not to broadcast. The BBC normally expects to have two sources or definitive BBC confirmation from a BBC correspondent or source. At this point we had none. Then came another important piece of information. The AFP wire at 13.57 added that in addition to the first snap, the source was 'An AFP reporter at the scene'.

In giving details of the 23 bodies at the site of the missile attack – the latest wire added, 'The AFP reporter was able to see the bodies of the victims'. In the instant verification process these were two crucial pieces of information. We were wrestling with whether the incident had happened, whether the information was good, and whether our credibility/integrity would be maintained. Because we had a named witness I believed we should have broadcast at 2pm. My editor remained cautious; I believe wrongly. Other news organisations had the same information. They were starting to broadcast it. The story was running as common currency. By 14.15 the incident was in the public domain with the NATO briefing underway, hosted by Colonel Konrad Freytag the SHAPE spokesman, and Peter Daniel, on that day standing in for Jamie Shea. This was what happened next. A journalist familiar with the AFP story asked a question. 'I will come back to you tomorrow', Colonel Freytag said twice. '*Tomorrow*' – 24 hours from then. What a lousy, inappropriate instinct that remains central to military thinking within NATO in my experience. This was that moment of crisis; that bolt out of the blue. This was how the robohack with a satellite telephone and that new transparency disorientated NATO over 24 hours. NATO lost control of the information edge. The institutional information control and power and superiority it believed it had as of right was not there. Hence the destabilisation. Rumours v News. The pressure is now. The need in real time is now, or an hour or two. Not 24 hours.

So in the battle of real time versus information: where do you or we position yourselves/ourselves on the time line relative to that early moment of intense impact? What compromises do you make in the integrity of information in order to secure that high ground? There are worrying lessons here from the way the Monica Lewinksy scandal first unravelled publicly in the US in mid-January two years ago. One study concluded that 90 % of what was reported was rumours. Information v Rumours again. But who seems to care any more?

An excellent analysis for the Shorenstein Center at Harvard by the director and distinguished former TV correspondent Marvin Kalb provides devastating evidence that in real time we no longer have news or facts as many assume we have or should have. Instead there is New News, where 'lines (between fact and opinion) are blurred'; where a rumour becomes a sort-of

fact; where there is a 'maze of whispered talk and gossip' that is 'transformed into perceived truth'. This is the new uncomfortable conundrum in real-time information. It is the new and flawed nature of information in real-time. It is being pressed forward relentlessly by the technology, which is removing many of the filtering layers in the rush to secure the high ground. The new dilemmas are uncomfortable. Only the foolish will dare to dismiss them as irrelevant.