



# Cyber-Defence to the Fore

Robert Hewson talks to Air Chief Marshal Sir Stephen Dalton, Chief of the Air Staff, about cyber-defence

The UK's critical electronic infrastructure – be it within the Ministry of Defence or on a broader national front – is constantly being tested by forces from across the undefined borders of cyberspace. Air Chief Marshal (ACM) Sir Stephen Dalton, Chief of the Air Staff, is clear that the level of threat the UK faces is sophisticated, significant and will only increase. “We are under pretty regular scrutiny from those who mean us harm and those who are just trying to test the system,” he says.

Whether these ‘attacks’ come from organised groups or enthusiastic amateurs is less important than the need to assess and block any damage they might inflict. Without a broad-based effort that pulls together every relevant element from the defence forces, government agencies, national industry, major businesses and utility providers, the UK will be vulnerable to an increasingly sophisticated level of cyber-sabotage that could affect us all in decades to come.

ACM Dalton is also clear that some firm boundaries need to be defined for ‘cyber-operations’. Much of what is needed to keep UK networks safe is the commonsense application of proper procedures. There is no evidence yet that the UK's military structures have suffered any damage from the constant cyber-attacks launched against them.

Furthermore, ACM Dalton says that the language of warfare often brandished by would-be ‘cyber-warriors’ in academia or the media is unhelpful and lacks the necessary moral and legal foundations. The UK, he says, should be able to keep all its crucial networks bulletproof – but should not be out firing ‘cyber-bullets’ of its own until this groundwork is laid.

The term ‘cyber-warfare’ is common currency now, but ACM Dalton notes that, in using it, not everyone knows what they're talking about – or at least not everyone is talking about the same thing. “We are all, I think, still working to understand precisely what we mean by ‘working in the ether’ and what the cyber-environment really entails,” he explains. “We've had

systems that have been intercepted since William the Conqueror to Enigma and beyond. So is this something completely new or just an extension of the same issues we've had to deal with in the past? Any enemy will try to understand what you're thinking, to intercept your messengers, your signals, whatever – at any stage.”

What has changed most recently is that the risks and implications are no longer simply military ones, and that cyber has the potential to cross the line from espionage to sabotage. “What is fundamental,” says ACM Dalton, “is ensuring that people understand this is not just a defence issue. This concerns government, industry, commerce and banking – everything is involved now.”

“The WikiLeaks issue shows that anything connected to something else is a potential access point to systems or information that you may not want the opposition, whatever form that takes, to have.”

He continues, “I would say that 80 per cent of the capability we require here is good old-fashioned data protection and OPSEC (operational security). The other 20 per cent is a whole bunch of things – quite a lot is obviously down to the technology of your network. But the rest of it is nothing new. It just needs to be more rigorously enforced, because network access can have such powerful effects.”

“We need to have a clear understanding of what our systems do; what they're connected to; and where our different systems interconnect with these other elements of national infrastructure – and, in some cases, commercial infrastructure.

“Because that is the case, we are obviously quite reliant on industry these days to support not just the development of new capabilities, but to support us in the field on operations. Making sure that they put the priority on the defence and protection of their information that is relevant to us is equally part of our job here in defence.”

**“This is not just a defence issue. This concerns government, industry, commerce and banking – everything is involved now”**

## Money and resources

ACM Dalton praises the work done to date at places such as the Defence Communications Services Agency, the Government Communications Headquarters and the RAF's own Air Warfare Centre. The Centre's role is particularly crucial when it comes to defending the RAF's deployed networks – a key concern for ACM Dalton. “When you are forward in another part of the world, reliant on a different set of links, fundamentally you are more vulnerable. My particular focus is to make sure we have the right governance in place and the right structure to enable us to be as capable out there as we are back here.”



The UK's existing defensive systems do seem to be working. Asked whether damage has been inflicted by what he describes as "the constant pressure on our networks", ACM Dalton replies, "As far as we know, the answer is 'no'. We're pretty confident our systems have a relatively high level of robustness against the sort of attacking that has happened and goes on now."

He adds: "It's a constant battle to ensure that you are protected. It's a 24-7 business. So it's not as if it is all manageable: therefore, 'don't worry about it'. We are having to put a hell of a lot of effort, money and resources and some very clever people into providing the best protection we can. That is not something that is just a passive practice. It is a very active and very resource-intensive process."

But when asked if it is warfare, ACM Dalton quickly replies, "No. My strong feeling is that's the wrong way to look at it. It's the wrong concept of what we're about. Because that then starts to raise all sorts of questions about the remit of military and armed forces actions – and I think there is a long way to go before we are anywhere near having clear answers about that. Certainly as far as I'm concerned, our chief requirement is to understand what techniques are out there so we can ensure we can protect against them."

Treating cyber-actions as warfare, or as a cause of warfare, is something we are ill-prepared for and should not be too hasty to embrace. Such

questions, says ACM Dalton, raise "both a moral and legal argument leading to the potential of military activity. The moral [argument], society hasn't had yet – and government and politicians will need to debate that. It's a very interesting area and I think there are some quite important moments coming when that has to be thought through."

#### **The moral and legal debate**

"What is an action within the cyber/ether that constitutes enough grounds to go to war? And what kind of cyber responses to that action are legal and proportionate – especially given the uncertainties about possible consequences on internet-based systems? Well, that needs to be thought through, not just nationally but internationally as well. As a head of an armed force, I'm very clear that we have to have a legitimate and legal basis on which to commit armed forces to war – whether in the traditional joint campaign, or in cyberspace."

"There is a requirement to understand what it means in terms of armed conflicts, and so forth. It's an area where, of course, I recognise a conflict in which both sides use cyberspace for sophisticated, integrated offensive action is entirely possible, and somewhere it may come – but we're not there yet." ■