Open Source takes flight in Defence World

William Payne

Trafalgar class SBMS: Britain's nuclear deterrent depends on Open Source

When Open Source Software first appeared on the scene in the late 1990s, many Government departments and public agencies were interested. The association of the word "Free" had much to do with it. Cost-conscious public bodies saw a way of saving money by simply switching software packages.

The interest of cash-strapped local authorities and public bodies in "free" Open Source was easy to predict. What few anticipated was the sudden surge of interest in Open Source from the defence and security community: Open Source appeared the antithesis of what military and security services would seek in their software.

When it became apparent that "free" meant "free to adapt and change", not "free" as in "no cost", the interest of many public bodies waned. Maintaining Open Source in practice could be demanding, and sometimes more expensive, than well established commercial alternatives. But while most public bodies turned their attentions to other ways of saving money on their software, the defence and security services' interest in Open Source has grown and grown. Indeed, while big budget public agencies like the Department of Works and Pensions and the NHS Connecting for Health have become bastions of proprietary software, Open Source looks set to become the de facto standard for all defence software, from logistics systems, through command and control systems, to embedded software in the latest fighters and missiles.

"Open Source is everywhere in defence", says Richard Easton, director of Global Defence Solutions at vendor Sun Microsystems. "From logistics systems, through command and control systems, to embedded systems, there's a tremendous enthusiasm for Open Source throughout the defence community. And the major security agencies are also major adopters of Open Source."

In Britain, examples of Open Source implementations include the Atomic Weapons Establishment, responsible for designing and maintaining the UK's arsenal of nuclear weapons and the MoD Defence Academy. The security services and GCHQ are reputed to be amongst the biggest users in government.

Europe's other big military power, France, is a big fan of Open Source. The French ministry of Defence is running

Published: Government Computing

William Payne is a writer on technology and business

07722 574085
williamhpayne@gmail.com
payne.writing.googlepages.com

a number of Open Source projects. Outside Europe, India, Singapore and Australia have all made major investments in defence Open Source. China is also un

But the biggest player in defence Open Source is the US military. The US defence establishment has broken new ground with its adoption of Open Source. The US uses Open Source throughout its entire defence infrastructure, including office systems, electronic surveillance, command and control and even the latest strategic weapons systems.

Examples of key US weapons systems using Linux include the THAAD Theatre High Altitude Area Defence Missile System programme, the next-generation F-35 Joint Strike Fighter, FCS and Land Warrior. THAAD is the US effort to shoot down incoming ballistic missiles. After three failed trial attempts in a row, contractor Lockheed Martin selected RedHawk Linux for the interceptor missile system in 2005. On January 27 this year, THAAD successfully shot down a dummy ballistic missile fired by the US from the other side of the Pacific.

The F-35 Joint Strike Fighter is the $250 billion next-generation fighter programme that will equip both the US and British air forces. Its panoramic cockpit display systems will be powered by LynuxWorks' real-time LynxOS Linux. Land Warrior and Future Combat Systems (FCS), both key components in US Network-Centric Warfare plans, will both be based on Linux. In 2003, a survey by MITRE, the US defence research coordinator, found over 250 computer projects within the US Department of Defense deploying Linux. Today, that number is likely to be in the thousands. In August last year, the US Department of Defense adopted the Advanced Systems & Concepts Roadmap Plan, which lay out a plan to adopt Open Source in every area of operation.

RedHawk Linux is a key component in the THAAD anti-ballistic missile system

The move to adopt Open Source is a result of the end of the Cold War. Before the fall of the Berlin Wall, every Nato unit had a carefully scripted role in the wider battle plan that had been developed over decades by Nato planners. Moreover, each service was largely standalone: the Royal Navy was tasked to tackle Soviet submarines coming out of the Kola Peninsula into the GIUK gap in the North Atlantic; the British army was tasked to defend northern Germany, and the RAF was tasked to defend the UK.

That careful script has been replaced by fluid operations that combine different forces from week to week. US, British, Australian and other forces can find themselves in operation anywhere around the globe, in any combination of services. The Royal Navy is moving from being a service dominated by Cold War frigates to a two supercarrier battlegroup with global force projection.

The name for this new approach is Coalition Warfighting. And it is Coalition Warfighting that is the principal driver for the adoption of Open Source in defence. Coalition Warfighting demands new Command, Control, Communications and Computers (C4ISTAR) that can easily integrate the command and control systems

of all units within a coalition force. Pulling all these different coalition technologies together, from logistics and admin systems through to fire control and target acquisition systems, is the Network Centric Warfare (NCW or NEC) infrastructure. This is the battlespace information grid that links all the disparate information and embedded systems together.

GCHG at Kelsey: the security agency is amongst the biggest users of Open Source in the UK

"We saw in the Gulf War how Network Centric Warfare was going to work," says Easton. "And it did work. It worked stunningly: it surprised everyone how well the theory worked in practice. But to make it work, and extend it even further, which means sharing information on a much larger scale than we've ever done before, from all sorts of discrete and embedded systems, then you've got to go to an Open base. You just can't do it any other way."

Another major impetus towards Open Source has been the move to replace expensive bespoke hardware with much cheaper commercially-available off the shelf systems (COTS). According to Michael Codner, Director of Military Sciences at the Royal United Services Institute, the shift to COTS is increasing, and so will the move to Open Source. "The COTS share of procurements particularly in IT has burgeoned and will continue to do so," he says. "I would expect Open Source to provide most of the COTS benefits and would have particularly useful employment in projects and programme subject to incremental acquisition – which includes a large proportion of IT and C4ISTAR projects."

Sun's Easton agrees that the ability to use COTS hardware and avoid either lock-in or obsolescence is a major factor. "There can be a real difference between commercial and military product generations. A proprietary commercial platform might have a planned product life of between three to five years. The military might plan to use a system for 15 to 20 years. The only way to employ COTS hardware to military time scales is with Open software."

However, RUSI's Codner sounds a warning note about security. "If source codes used in weapon, surveillance, and operational information fusion and communications network systems, are easily available to potential opponents, they may be able to create disruptive devices. The UK and other major military powers will be increasingly dependent on networked military capability and the network itself is an obvious node of vulnerability. The issues of redundancy and reversionary procedures in the event of a disrupted network have not, I feel, been fully thought through in the gallop towards NEC."

The move towards Open Source has not gone without challenge. The most notable opponent has been embedded software specialist Green Hills chief executive Dan O'Dowd. He has labelled Open source "an urgent threat to our national security". Microsoft's Jerry Fishenden, National Technology Officer at Microsoft UK, takes a more balanced view of the pros and cons of Open Source. "The important issue is ensuring the right people have the right tools for the job. It is not about an abstract ideological discussions of software development methods," says

Fishenden. “Choice is important. Like any other customers, military customers need to select appropriate software based upon a wide range of factors. Whether that is closed source, open source or any hybrid combination. The decision about whether to adopt any particular type of software is rightly one for the MoD to decide, based on a range of factors including value for money, operational support, integration, security, and ability to fulfill the mission.” Microsoft software, Fishenden says, has “a proven operational capability in the most demanding of environments. And a proven ability to support timely, integrated information - whether for operational use in theatre or in the fixed base.”

Meanwhile, the Open Source vendors are busy expanding their share of the profitable defence market. And Open Source doesn’t just mean Linux, or Linux applications. Sun Microsystem’s Solaris, which is a major platform in military mission-critical systems throughout NATO, is also an Open Source system.

Hewlett-Packard, which is also a major defence industry vendor, is a leading Linux vendor, not just on the company’s commodity platforms, but also on its large scale servers, as an alternative to HP-UX. HP also sells the Tandem range of NonStop computers, based on fail-safe parallel mainframe technology. NonStop forms the basis for the US Department of Homeland Security’s information systems, and other security systems. HP recently formed a coalition of universities to migrate NonStop to a specially adapted version of Linux.

Silicon Graphics is another company selling Linux systems to the military, recently selling a 2,048 processor Linux supercomputer to the US Department of Defense for advanced weapons design and weapons test simulations.

Specialist Linux vendors are also making inroads into the defence market. Linux Networx recently sold five Linux supercomputers to the US Department of Defence, in an installation that will provide 80 Teraflops performance, which will be used for biological and chemical warfare simulations.