

Using Commercial Software in Defence and Mission-Critical Systems



Are your **people**  **ready?**



Microsoft[®]

Introduction

The past two decades have seen a fundamental shift in the way defence organisations around the world operate. Galvanised by incidents such as 9/11 and the rise of terrorism as an all-pervasive global threat, military organisations have had to plan and react with faster tempo. To do so has required not just a shift in tactics, strategy and operations, but also in the underlying technology that enables defence forces to successfully combat the changing nature of threat.

As early as 1997, U.S. Chief of Naval Operations, Admiral Jay L. Johnson, publicly identified "...a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare,"¹ later defined by Alberts, Garstka and Stein as "...an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision-makers and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability and a degree of self-synchronization."²

Put differently, Network-Centric Warfare (NCW) is a command system that translates the rapid and secure sharing of information into combat superiority. NCW enables military organisations to share intelligence and information, process it and then react to it in a timely manner, up and down the command echelons.

Born from the need to provide relevant information in real time or close-to-real time, NCW has in turn raised the bar on how mission-critical Command & Control (C2) systems operate. Modern C2 systems have effectively evolved into all-encompassing Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems, able to provide critical information to inform decision-making of commanders and units on the ground. As a result, the criteria to be considered when evaluating the quality of a C4ISR system, according to Alberts, Garstka and Stein, is "...whether changes in circumstances are noted and how quickly they are noted, as well as the appropriateness and timeliness of response".³

Providing this level of responsiveness requires interoperability between C4ISR systems so that data can be securely shared, as well as secure collaboration capabilities that enable quick and effective communication of commands. Successful C4ISR systems also need to be adaptive and flexible to support rapidly changing operational conditions and ensure interoperability with multiple alliance partners with minimal integration complexities. The increasing role of unmanned aerial vehicles and other types of sensors is just one example of this interoperability requirement.

In the light of these sophisticated requirements, this paper considers the merits of leveraging Commercial Off The Shelf (COTS) technologies for NCW and C4ISR systems, specifically in relation to how COTS can help reduce the complexity and risks associated with building mission-critical systems. It also examines common misperceptions between Commercial Software (CS) and Open Source Software (OSS).



"...a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare."

Admiral Jay L. Johnson
U.S. Chief of Naval Operations (CNO), USN

Choosing technology providers in the information age

The uptake of COTS-based NCW technologies among defence organisations has been driven by a number of key trends. Firstly, a proliferation in the quantity and variety of information to be gathered and processed has prompted a move towards standards-based NCW systems. Among other benefits, standardisation makes it appreciably easier for systems to interoperate and share information.

Secondly, military organisations have sought to leverage the rapid and continual advances in COTS-based systems made by commercial companies who invest substantially in Research and Development. Successful military organisations have therefore gained tactical advantages by integrating continually improving features and capabilities into their NCW systems.

Thirdly, the rise of coalition-oriented operations and emergency relief operations has catalysed wider support of COTS-based systems, because information now needs to be shared with other government agencies and Non-Government Organisations (NGOs) outside the traditional unit and allied forces. Using a COTS-based system, connections between entities can be set up simply and easily, and training is usually minimised due to the familiarity of the interfaces.

Finally, CS based systems are usually more cost-effective than their open source counterparts when Total Cost of Ownership (TCO) is taken into account. OSS systems may include an up-front annual subscription fee based on the number of computers, resulting in similar initial procurement costs to a CS system, but a true cost benefit analysis must take into account staffing, training downtime, outsourced functions support and ongoing management. The 2008 Jane's Report, *Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles*, acknowledges that: "While the initial cost of procuring CS in most case is higher than OSS, the lower procurement cost of OSS is ultimately only a fraction of the cost that OSS users are likely to incur. Administrative and support costs, such as those incurred transitioning from a CS system, training on difficult-to-navigate interfaces, obtaining software support through downtime of systems as patches are released, integrating OSS and high-end CS applications, and managing the software all contribute to the cost of an OSS procurement."⁴

Defence organisations recognise that the cost of migration and support should always be considered as part of the total cost of choosing the product and that suitably skilled and trusted manpower needs to be available to support the software platform. Further weighing in the favour of CS applications is the ecosystem of independent software vendors and skilled systems integration partners available to develop and deploy mission-critical C4ISR systems, providing military organisations with choice and ongoing support options.



"While the initial cost of procuring CS in most case is higher than OSS, the lower procurement cost of OSS is ultimately only a fraction of the cost that OSS users are likely to incur."

The Jane's Report, 2008

Microsoft solutions in defence

To support these demanding NCW requirements, modern military organisations are turning to Microsoft (and its worldwide partner network) to provide solutions that interoperate within a descriptive architecture and reference model – or the 'Connected Government Framework': Microsoft's standards-based architecture facilitates information-sharing and collaboration at the highest security levels.

Microsoft *Situational Awareness* solutions, for example, will aggregate and analyse multiple sources of data and information to give military personnel an accurate, real-time visualisation of the battlefield, regardless of physical limitations. This enhances the Command and Control decision-making process by helping personnel understand rapidly changing conditions, execute operational plans, and prepare for future operations. These solutions also enable secure real-time communications, including mission planning and orders dissemination, messaging and data transfer.

Around the world, Microsoft *Military Messaging* solutions are the foundation for systems that enable defence organisations to issue formal communications with speed and ease, leveraging the familiar Microsoft interfaces and any existing Microsoft infrastructure. Official reports, notices and other information can now be sent with integrity, confidentiality and delivery. All messages are fully auditable and can be archived for up to 30 years. Microsoft partners' *Military Messaging* solutions include precedence levels (Routine, Urgent, Priority, Immediate, Flash), security classification levels (Unclassified, Confidential, Secret, Top Secret), role-based delivery and fire-and-forget guaranteed delivery. Microsoft's Unified Communications enables military-specific Microsoft® Office LiveMeeting, chat, video conferencing and white board collaboration.

Microsoft state-of-the-art Command and Control solutions provide:

- Better interoperability for Command and Control processes, enabling enhanced collaboration across multiple theatres of operation and coalition forces – even in bandwidth-constrained environments.
- Seamless operations across a wide variety of communication methods and devices – important when the geographically dispersed forces are using radios, GPS devices and other sensors from different manufacturers to communicate and enhance situational awareness.
- Scalable, secure and connected solutions based on open standards architecture designed to support databases and communications networks across defence agencies and NGOs.
- Easy-to-use applications, tools and technologies backed by multibillion-dollar research and development⁵ initiatives focused on driving innovative, customer-focused development of future products.

Built using the Microsoft® .NET platform, FusionNet is a distributed system deployed by the U.S. Army to disseminate 'ground truth' intelligence and unit management information throughout the battlespace.

Before FusionNet, battlefield event information was scattered among numerous Army systems and databases, which couldn't communicate with one another. Now information can be provided vertically among echelons and horizontally across functional areas and organisational boundaries in real time giving military personnel shared situational understanding. Furthermore, the use of a smart client distributed architecture helps ensure that FusionNet can scale from today's disadvantaged tactical network environments as well as on future military Global Information Grid networking environments.



Microsoft technology in Network-Centric Warfare

"As the new version of FusionNet is implemented throughout the current theatre of operation, we expect the data capture rate and, more importantly, the information availability rate for battlefield events to increase to 75 percent or more, an improvement of more than 1,500 percent."

Major Kurt Warner,
Knowledge Management Officer for
the U.S. Army XVIII Airborne Corps and
Multi-National Corps, Iraq G-6

Why are defence organisations choosing Microsoft over Open Source?

There are several key differences between Commercial Software (CS) and Open Source Software (OSS) that warrant careful comparison. The most obvious contrast between the two approaches is that OSS allows the original source code of a program to be made freely available to the public for perusal, modification and redistribution, provided these modifications are openly shared with the wider user community whereas CS is created by certified, commercial developers. Over the past few years, a series of critical considerations has motivated military organisations to adopt Commercial Software for their mission-critical deployments.

Foremost has been the issue of risk, leading to a preference for secure, known options from a pedigree of trusted providers. According to the 2008 Jane's Report, *Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles*, security and supportability was the rationale behind the British Ministry of Defence decision to buy Microsoft® Windows® for their UK submarines. Similar reasoning went into Israeli defence company Elbit's decision to engage Microsoft from the outset.

The issue of familiarity and operating system ease of use is also an important motivator towards CS, with organisations seeking to leverage existing infrastructure and minimise staff training in new technologies. According to Jane's, when the Royal Netherlands Army (RNLA) created a range of state-of-the-art IT awareness and C2 support tools based on a Microsoft® Windows Server System™, "Among the many factors considered by the RNLA was the easy-to-use and manage infrastructure and the lack of training required to become familiar with the tactical messaging systems (TMS)."⁶

Israeli defence manufacturer, Elbit Systems, also entered a strategic partnership with Microsoft in which Microsoft would develop a platform consisting of Microsoft Windows, the Microsoft .NET Framework, and Microsoft® SQL Server®, on top of which Elbit Systems would install proprietary C2 software. In evaluating whether to use OSS or CS for their C2 architecture, Elbit Systems weighed up a number of key factors including the ease of integration among different layers of the C2 hierarchy, the costs associated with having to hire and/or train in-house engineers familiar with OSS software, the issues of support throughout a long life cycle and, ultimately, the fact that Microsoft could provide multiple products with single-vendor convenience. According to Yosefa Abramovici⁷, Director of Unmanned Air Vehicles (UAVs) Systems Division: "With the new infrastructure, our development team can build and integrate applications more quickly."

She also said: "With a more flexible software development kit, our customers can build their own applications on top of their infrastructures without releasing sensitive defence information to outsourced companies."

Elbit Systems is representative of the breadth and depth of expertise that is available through Microsoft's global ecosystem of independent software vendors and systems integration partners. This broad defence partner ecosystem with the experience and capabilities to develop and support mission-critical C4I systems is a compelling draw card for military organisations looking to leverage choice and competition when selecting solutions and suppliers. Furthermore, Microsoft has a well-resourced partner program dedicated to providing ongoing skills development, training and accreditation, helping to ensure the highest standards among its partner network.



"...security and supportability was the rationale behind the British Ministry of Defence decision to buy Microsoft Windows for Warships for their UK submarine ship."

The Jane's Report, 2008

The Security Debate

Arguments between CS versus OSS in the area of security focus on a number of assertions from the development perspective. Proponents of OSS argue that open source is inherently more secure than CS because of the 'many eyes' concept. This theory argues that OSS solutions, with their source code available for public scrutiny, are inherently more secure than commercial software solutions on the basis that teams of developers will take the time to analyse and review the source code prior to using it. However, this argument does not take into account the propensity of OSS teams to do so, given the volumes of OSS code available. Director of Software Policy at Business Software Alliance (Asia), Goh Seow Hiong, comments: "It is not realistic to expect that every single line of the code has been scrutinised by a wide range of security experts,"⁸ going on to conclude that: "Given such a scenario, it appears premature to declare that open source is superior in security."

Naval Professor, Simson L. Garfinkel, also explains that: "While this [many eyes] theory sometimes works, mostly it's wrong. Sometimes the eyes just aren't looking, even though the source code is readily available; sometimes the eyes that are looking aren't properly trained; and sometimes the eyes find what they are looking for – except the eyes are working for the enemy."⁹

Garfinkel's concern is that the very openness of Open Source can also constitute a security risk as the code is more transparent to those with malicious intentions. Keen OSS advocates will argue that attacks on the software should be considered part of the software development process; however, the 2008 Jane's Report concludes: "This is perhaps OSS advocacy taken one step too far into the realm of near tautology – a system's invulnerability is enhanced and even proven by its having been breached."¹⁰ Ultimately, a system by which improvements are made after suffering security attacks must be given serious consideration in a military context.

In a similar vein, senior military officials are "...uncertain of what to make of OSS solutions and their relevance and acceptability in the highly classified and high stakes context of emerging C4I systems and platforms." It would be difficult to implement a wholly OSS system in a military environment, where so much of the information within the system needs to be highly classified. Jane's Report also notes that OSS is "a bit of a headache for IT people," largely because, while increasing the number of individuals reviewing the code is accepted as a positive development, allowing everyone to view the source code creates challenges and uncertainty in military IT communities.¹¹



"...it appears premature to declare that open source is superior in security."

Goh Seow Hiong
Director of Software Policy,
Business Software Alliance (Asia)

The Security Debate

The viability of the 'many eyes' theory was also exposed by researchers at Purdue University who discovered a devastating bug in the Kerberos Version 4 random number generator that had been developed at MIT and distributed to the open source community. Dozens of companies had incorporated the source code into their products without any scrutiny and were consequently exposed to a serious security vulnerability that enabled intruders to masquerade as authorised Kerberos users and gain access to services and resources not intended for their use.¹²

In May 2008, a similar error was discovered with the realisation that, in 2006, a few programmers working on an open source security project changed two lines of code, which had created profound security vulnerabilities in at least four different open source operating systems, 25 different application programs, and millions of individual computer systems on the Internet.¹³

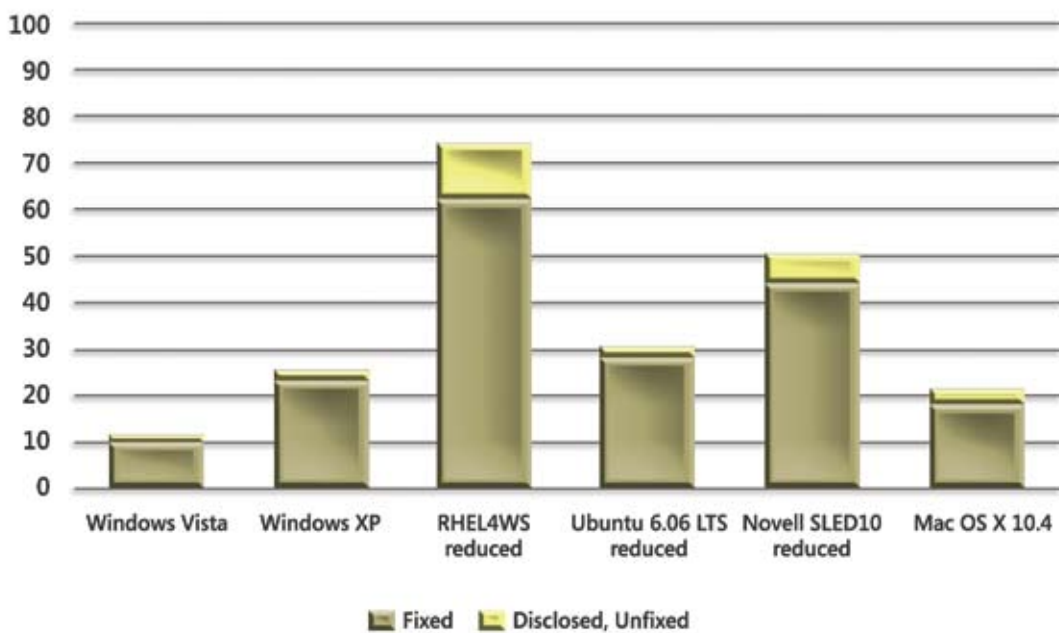
The concern over the availability of source code for the purposes of undertaking a security review has also been largely addressed by CS vendors, such as Microsoft, who provide governments with access to their source code through their Government Security Program (GSP). Qualifying governments¹⁴ are granted zero-cost, online smartcard access to source code for the most current versions, beta releases, and service packs of its high-volume software products¹⁵ as well as access to cryptographic code and development tools. The GSP also provides transparency through disclosure of Microsoft technical information. This engineering-level view of Windows architectural design as it relates to security provides development teams with greater insight regarding the platform's integrity, enhancing their ability to design and build secure computing infrastructures in a military context.

Proponents of OSS have also argued that it is easier to detect and remediate flaws in software whose source code is published as the very openness of their process leads to the rapid release and sharing of fixes and patches. However, recent statistics in the six-month Windows Vista® vulnerability report (see over) reveal that it is CS software vendors with their teams of developers devoted to detecting and fixing software errors who may be more effective at disclosing and fixing vulnerabilities. To achieve security assurance, Microsoft mandates a process called The Microsoft Security Development Lifecycle (SDL) throughout the development process. This has led to measurable and widely recognised security improvements in Microsoft products such as Windows Vista and SQL Server. In the spirit of supporting a more secure and trustworthy computing ecosystem, Microsoft also makes SDL process guidance, tools and training available to development teams and to customers and partners.

The Security Debate

Given that Microsoft COTS software provides both selective openness to qualified government organisations and a highly rigorous assurance program, backed by a global security response centre that provides scheduled security bulletins, patches and updates, it offers strong appeal to developers in the military context, particularly when contrasted with the ad hoc nature of remediation in the OSS environment. This innovative hybrid approach to software development is allowing Microsoft to leverage the advantages of both methods, ultimately benefiting both consumers and developers.

Vulnerabilities – Reduced Linux Builds – First 6 Months Fixed & Unfixed – High Severity Only



This chart shows high-severity vulnerabilities during the first 90 days of availability, broken down by vulnerabilities fixed and vulnerabilities unfixed. **Windows Vista continues to show a trend of fewer total and fewer high-severity vulnerabilities at the 6-month mark** compared to its predecessor product Microsoft® Windows® XP (which did not benefit from the SDL) and compared to other modern competitive workstation Operating Systems.

* Note that this chart is showing the reduced Linux builds that exclude non-default and optional components without equivalents on Windows. To read the complete report, visit http://blogs.csoonline.com/windows_vista_6_month_vulnerability_report

Interoperability and Open Standards

Virtually all software companies have acknowledged the need for interoperability in today's technology landscape, prompted in part by the standards-based nature of the Internet. Standardisation for interoperability enables consumer flexibility in selecting from a range of competing software products. To foster the development of interoperable software, open standards provide guidance as to how data and information may be exchanged between discrete software components operating together. Open standards are often confused with open source, thanks to their similar-sounding names. The difference is that open standards are defined and decided upon by a set group of collaborators. Once defined, open standards are available to any software developer, and they do not require open source software for their adoption or use. The best example of open standards at work is the Internet – virtually all of the technology specifications it depends on are open, as is the process for defining new ones.

Open Source, however, involves software developers being allowed to individually decide the manner in which they code software and allows them to distribute modifications and derived works as long as the source code is also available.

In response to widespread consumer demand, software industry players are already working together to define open standards for interoperability. The upshot of this is that standardisation of basic software functions will shift competition to the advanced application levels. Goh Seow Hiong summarises this dynamic, explaining that: "Vigorous competition among different, but interoperable, technological products will allow customers to exercise free choice among innovative products to select the solution that best serves their needs. The undue preference for one particular product, platform or software licensing or development model not based on objective criteria such as open standards will inevitably disturb the competitive forces that can bring about the best results for consumers."¹⁶

Ultimately, the software industry has a responsibility to come together to address the interests of users in interoperability and effective data exchange, both for the benefit of the consumer and the advancement of software technology as a whole.

No one is addressing open standards more diligently than Microsoft, with its leading interoperability principles making it a "prime example" of open standards at work, according to the 2008 Jane's Report. "Microsoft [has] engaged the OSS community in a fashion that tries to bridge the gap between OSS and CS. This evolving hybrid approach attempts a synthesis of 'open' principles coupled with the benefits afforded by a central commercial entity. Microsoft has made a concerted effort to realise this approach by opening up their operating systems and programming frameworks to the greatest extent possible without compromising their intellectual property."¹⁷

Microsoft holds a particularly important position in the software industry, owing to daily and critical use of its products by customers the world over. Certain Microsoft products, such as Windows Vista, the Microsoft .NET Framework, Microsoft® Windows Server®, Microsoft SQL Server, Microsoft® Office, Microsoft® Exchange Server, and Microsoft® Office SharePoint® Server, have become so central to operational continuity of businesses and government organisations that interoperability and data portability solutions are becoming inextricable from Microsoft's software development.



"Microsoft has made a concerted effort to realise this approach by opening up their operating systems and programming frameworks to the greatest extent possible without compromising their intellectual property."

The Jane's Report, 2008

Interoperability and Open Standards

Microsoft's stance on standards-based interoperability is defined in its four core principles:

- Microsoft is committed to establishing and maintaining open connections between its high-volume products and non-Microsoft products. Software is usually designed to interoperate via external protocols or application programming interfaces (APIs), and Microsoft will be keeping these connections open so that any developer may connect to Microsoft products. Microsoft is also publicly disclosing documentation for open protocols and open APIs on its company Web site.
- Microsoft is aiming for broad compatibility with other major standards implementers by supporting the relevant standards that promote interoperability. Microsoft actively participates in standards bodies, such as the Interoperability Executive Customer Council, and publicly documents how it adopts standards for the software development community. Overall, Microsoft contributes to, and collaborates with, more than 150 standards organisations annually.
- Motivated by the belief that consumers should be able to access data from Microsoft products in other software products, and vice versa, Microsoft is committed to using and supporting industry-standard file formats. This is accompanied by a commitment to continue designing its high-volume products with plug-in architecture that allows developers to incorporate support for other file formats.
- As no single company can address interoperability challenges on its own, Microsoft recognises that collaboration with customers, partners and other vendors is of critical importance. This collaboration includes open communication on the interoperability challenges that customers are experiencing and the ways in which those challenges can be addressed. Microsoft interacts directly with consumers and developers through its Web-based Interoperability Forum, as well as via its newly launched Document Interoperability Initiative, which brings together more than 30 partners and competitors to test interoperability between existing implementations of Open XML Format and the OpenDocument Format (ODF) on a variety of platforms and devices, including Mac OS X Leopard, iPhone, Palm OS, Symbian OS, Linux and Windows Mobile®.

Interoperability is the key to military operations where the latest technology is provided by a wide range of suppliers. No matter what kind of campaign is in play, military organisations will need to be able to establish themselves quickly in unfamiliar territory, with easy collaboration and communications between coalition forces, even if these allies have never worked together previously.

Described by some as a 'living architecture,' the Royal Netherlands Army (RNLA) has created a range of situational awareness and Command and Control (C2) support tools in a shift towards Network-Centric Warfare. Based on the Microsoft Windows Server System and other COTS technologies, this C2 framework has provided a common platform for all its applications.

"It's all about enabling Network-Centric Warfare," explains Col. Geerlof Kanis, Commander, Command and Control Support Centre, RNLA. "We are receiving contributions from Danish, German, Norwegian, French and Belgian battalions, each with their own Command and Control systems, so interoperability is very important for us. There are a lot of international military bodies promoting it."¹⁸

Several Microsoft applications such as Microsoft Theatre Independent Tactical Army and Air Force Network (TITAAN) and the Microsoft Battlefield Management System have already supported operations in Afghanistan and Iraq. The RNLA have also been working with the NATO Response Force (NRF) to create a multinational high-readiness and technologically advanced fighting force, combining elite land, air and sea units into a single, flexible force that can be deployed anywhere in the world in five days and sustain itself for up to a month on a wide range of missions.

"...interoperability is very important for us, and there are a lot of international military bodies promoting it."

Col. Geerlof Kanis, Commander, Command and Control Support Center, RNLA

The Support Bucket

The final concern in the evaluation of CS and OSS solutions in a military context is the issue of supportability. The past few years have seen a diminishing level of enthusiasm for OSS, prompted largely by disappointment over the lack of support OSS is able to provide in comparison to CS vendors, who can supply dedicated and tailored support over the course of a product's life cycle (which, in the military, could be for as long as three decades).

The 2008 Jane's Report confirms: "Some militaries that are being particularly aggressive and thoughtful in their approach to developing and implementing NCW-related systems and platforms have cited supportability as a key factor influencing their preference for CS [Commercial Software]."¹⁹

Lack of vendor support and the difficulty in testing solutions was found to be the largest obstacle when implementing OSS systems by Australian government agencies, as reported in a survey released by the Australian Government Information Management Office (AGIMO) in January 2008. "According to the CIOs of Australia's three largest government departments – Defence, the Australian Tax Office and Centrelink – support is a very real concern – the central reason why more open source is not widely used in government."²⁰

When troubleshooting an OSS system, users can only turn to a wide and disparate community for support, usually via online forums. Not only is there no guarantee that a problem can be solved quickly and effectively using this method, but there is also no verification whether individuals on forums are knowledgeable or well-meaning.²¹

In a military context, time is a precious commodity, meaning it is far more effective for personnel to use a CS-based system with a central authority that is able to provide dedicated support, such as Microsoft Services.

Microsoft Services operates 24 hours a day, seven days a week, providing rapid-response support coverage for all its available software and infrastructure systems, including critical situation management and on-site assistance as needed. Microsoft Services also provides proactive strategies for maximising the availability and efficiency of infrastructure, risk assessment and reduction, improving processes and boosting the productive use of Microsoft technology.

It is for these reasons that the British Ministry of Defence (MoD) uses Microsoft products to keep its Microsoft infrastructure well-oiled and maintained. For the past four years, the MoD has relied on Microsoft Services to provide accountability, ease of use, security and scalability. Microsoft enables the MoD to effectively coordinate the highly specific needs of its operations, and ensure that defence forces can collaborate with their allies as well as with a vast partner system, using tools and best practices within a wide range of consulting competencies.

The issue of familiarity is akin to supportability as military technology is always quick to change and develop. Frequent advances in technology leave defence forces little time to train on new software, especially if they are on the move in remote locations. An easy interface, then, becomes integral to maintaining an effective, state-of-the-art military that can focus on the job it does best – serving the nation, not the needs of software companies. Thus operating system ease of use is becoming an increasingly important factor when deciding between software options.



"...Some militaries that are being particularly aggressive and thoughtful in their approach to developing and implementing NCW-related systems and platforms have cited supportability as a key factor influencing their preference for CS [Commercial Software]."

The Jane's Report, 2008

Conclusion

As military organisations make the transition into Network-Centric Warfare and evaluating the use of COTS software systems, there has been much deliberation over the suitability of Open Source software (OSS) solutions versus Commercial Software (CS) solutions. As this paper has demonstrated, while there is an important place in the software industry for OSS principles, defence agencies around the globe have not adopted OSS over COTS technology. Given the sophisticated need for a networked awareness of field data, mission-critical intelligence and changing commands in real time, within an exceptionally secure framework for private collaboration and strategy, military organisations are turning to CS-based systems.

CS-based systems provided by dedicated vendors like Microsoft offer a solid framework for cutting-edge C4ISR systems, which are instantly interoperable with both existing and yet-to-be-implemented software components. Microsoft software takes advantage of the best aspects of OSS systems, by offering software that reflects industry-standard interoperability principles along with enough transparency for developers to create and install their own plug-ins whilst still maintaining the highest security levels. The Microsoft Government Security program also provides transparency through the disclosure of Microsoft technical information to qualified GSP participants. This view of Windows architectural design provides an engineering-level view of the platform's integrity and enables military organisations to design and build more secure computing infrastructures. Moreover, Microsoft Services offers dedicated all-hour support, facilitating usage of a C4ISR system with maximum productivity and cost-effectiveness. Perhaps most importantly, all of these benefits do not come at the cost of cyber-terrorist vulnerability, as source code is only ever made available to authorised personnel and security is not reliant on outsider attack in order to evolve. The 2008 Jane's Report notes that the Microsoft hybrid method has "...found resonance in the military C4I environment and has demonstrated an ability to address the specific concerns and priorities (trust/pedigree, supportability, ease of use, deferred risk) that are of utmost concern to many military decision-makers."²²

Microsoft C4ISR solutions have already been deployed in a large number of military organisations in Asia, Australia, the Middle East, Europe, the United States and Canada. Furthermore, most Systems Integrators, including Lockheed Martin, Raytheon, Elbit, Northrop Grumman, Saab, Thales, EADS, BAE and Systematic have also adopted the Microsoft platform in their C4ISR solutions. For example, Microsoft products, most notably the Theatre Independent Tactical Army and Airforce Network (TITAAN) system – an integrated network that supports all data and telephony communications within disparate operational command posts – has enabled the RNLA to create highly mobile military units with equipment that is easily transportable and reduced to a bare minimum. The TITAAN solution also received international acclaim at the U.S. Network-Centric Warfare Awards, winning the 2004 award for best program/initiative from a coalition partner.



Conclusion

Israeli Defence company Elbit has developed a C4ISR system that utilises Microsoft products for its entire system hierarchy. Not only has Microsoft provided a swift and easy software integration among the different layers of the C4ISR echelon, but it will continue to maintain and support the system throughout a long life cycle with single-vendor convenience.

Even though OSS has been trialled and will continue to operate within military organisations, since a military context “stresses supportability, ease of use, deployability and restricted communities”, there are ultimately more reasons to trust a COTS vendor like Microsoft. The 2008 Jane’s Report concludes: “Several militaries that are pursuing transition to a more Network-Centric Warfare aggressively (Australia, the UK, Israel, the Netherlands) have sought to solidify their relationships with CS providers.”²³

The lack of support (especially in the long term) coupled with frequent downtime and self-maintenance render OSS an unreliable option in the military. For organisations ready to make the leap into hyper-modern Network-Centric Warfare, however, Microsoft is quickly becoming the premier choice, backed by its multibillion-dollar research program, user familiarity and ease of use, rapid deployment time and cost-effective software interoperability. Perhaps the choice is better posed this way: “When choosing a new solution to help you adapt to the changing nature of modern warfare, do you really want to work harder, or smarter?”

In summary, Microsoft COTS for defence provide three unassailable benefits over OSS.

1. Security: In addition to sharing source code through its Government Security Program, Microsoft protects governments with a well-resourced, formal program to address vulnerabilities in its software using a proven and successful methodology. In comparison, OSS can be dependent on ad hoc initiatives from uncredentialed developer forums in response to issues, usually after the fact.

2. Interoperability and Open Standards: Aware that military solutions need to interoperate with a wide range of existing solutions and specialist systems, Microsoft supports open standards and industry-standard file formats to promote interoperability. Most products are specifically designed with plug-in architecture, support for other file formats and external protocols or application programming interfaces (APIs). Microsoft also publicly discloses documentation for open protocols and open APIs on its Web site and collaborates through industry forums with customers, partners and other vendors to promote interoperability between emerging systems.

3. Support: Unlike the break-fix support which often characterises the OSS environment, Microsoft has a global network of trained, professional partners who offer proactive assistance and the transfer of knowledge and skills to military IT personnel. Furthermore, Microsoft Services operates 24 hours a day, seven days a week, providing rapid-response support coverage for all its available software and infrastructure systems, including critical situation management and on-site assistance as needed. Microsoft Services also provides proactive strategies for maximising the availability and efficiency of infrastructure, risk assessment and reduction, improving processes and boosting the productive use of Microsoft technology.

“Several militaries that are pursuing transition to a more Network-Centric Warfare aggressively (Australia, the UK, Israel, the Netherlands) have sought to solidify their relationships with CS providers.”

The Jane’s Report, 2008

Bibliography

Primary

"Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles", *Jane's*, 2008.

Alberts, David S., Garstka, John J., Stein, Frederick P.,
"Network Centric Warfare" 2nd Edition, CCRP Publications, 2002.

Garfinkel, Simson L., "The Security Of Open Source Software," *CS Online*, 7 July 2005.

http://www.csoonline.com/article/220441/The_Security_of_Open_Source_Software_/1

Garfinkel, Simson L., "Alarming Open Source Security Holes: How a programming error introduced profound security vulnerabilities in millions of computer systems", *Technology Review*, 20 May 2008

<http://www.technologyreview.com/Infotech/20801/?a=f>

Hiong, Goh Seow, "Open Source vs Commercial Apps:
The Differences That Matter II" *ZDNet Asia*, 1 October 2004,

<http://www.zdnetasia.com/insight/hardware/0,39043471,39195509,00.htm>

Johnson, Admiral Jay L., Chief of Naval Operations (CNO), USN, Address at the U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, in Annapolis, Maryland, on 23 April 1997.

Tung, Liam, "6 months vulnerability report for operating systems:
Open Source barred from Australian government," *ZDNet Australia*, 1 April 2008;
http://blogs.csoonline.com/windows_vista_6_month_vulnerability_report

Secondary

Overly, Michael, "Open Source; Is It Inherently More Secure Than Proprietary Software?"
CS Online; *Overly on Security*, 20 February 2007.

http://blogs.csoonline.com/open_source_is_it_inherently_more_secure_than_proprietary_software



Footnotes

- ¹ Adm. Jay L. Johnson, Chief of Naval Operations (CNO), USN, in his address at the U.S. Naval Institute Annapolis Seminar and 123rd Annual Meeting, in Annapolis, Maryland, on April 23, 1997.
- ² David S. Alberts, John J. Garstka & Frederick P. Stein, *Network Centric Warfare* (2nd Edition, CCRP Publications, 2002), p. 2.
- ³ Ibid., p. 43.
- ⁴ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 7.
- ⁵ In 2007, Microsoft spent US\$7 billion on software R&D
- ⁶ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 12.
- ⁷ Elbit Systems Defence Manufacturer Chooses Standards-Based Infrastructure and Simplifies Processes
<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000002374>, Microsoft 2008) p.1
- ⁸ Goh Seow Hiong, "Open Source vs Commercial Apps: The Differences That Matter II" *ZDNet Asia*, 1 October 2004,
<http://www.zdnetasia.com/insight/hardware/0,39043471,39195509,00.htm>
Hiong is the Director of Software Policy (Asia) for Business Software Alliance.
- ⁹ Simson L. Garfinkel, "The Security Of Open Source Software," *CS Online*, 7 July 2005.
http://www.csoonline.com/article/220441/The_Security_of_Open_Source_Software_/1
Garfinkel is an Associate Professor at the Naval Postgraduate School in Monterey, California, and a fellow at the Center for Research on Computation and Society at Harvard University.
- ¹⁰ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 14.
- ¹¹ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 12.
- ¹² Simson L. Garfinkel, "The Security Of Open Source Software," *CS Online*, 7 July 2005.
- ¹³ Simson L. Garfinkel, "Alarming Open-Source Security Holes: How a programming error introduced profound security vulnerabilities in millions of computer systems", *Technology Review*, 20 May 2008
- ¹⁴ Subject to such requirements as U.S. export approval – see
<http://www.microsoft.com/resources/sharedsource/Licensing/GSP.msp>
- ¹⁵ <http://www.microsoft.com/Presspass/ofnote/04-01-08GutierezIAMArticle.msp>
- ¹⁶ Goh Seow Hiong, "Open Source vs Commercial Apps: The Differences That Matter II" *ZDNet Asia*, 1 October 2004,
<http://www.zdnetasia.com/insight/hardware/0,39043471,39195509,00.htm>
- ¹⁷ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 8.
- ¹⁸ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 16.
- ¹⁹ Ibid p. 16.
- ²⁰ Liam Tung, "6 months vulnerability report for operating systems: Open source barred from Australian government," *ZDNet Australia*, 1 April 2008; http://blogs.csoonline.com/windows_vista_6_month_vulnerability_report
- ²¹ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 6.
- ²² "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 21.
- ²³ "Open Source Software in Defence Markets: Issues surrounding OSS Usage in C4ISR roles," *Jane's 2008*, p. 21.

Microsoft Services – Partnering for success

The aim of Microsoft Services, the consulting and support arm of Microsoft, is to help customers and partners innovate, connect and maximise their investment in Microsoft technologies. Microsoft Services has worked closely with a number of defence departments around the world, to help provide IT advisory and planning (ITAP) services, technology consulting and proactive support.

Microsoft Services ITAP helps customers identify and prioritise important defence capabilities and provide mapping into specific IT capabilities that need to be implemented or improved. ITAP consultants can help military customers gain a better and more comprehensive view of their existing technology. This helps defence organisations rationalise and optimise their IT investment.

The technology consulting service also provides access to proven best practices, methodologies and guidance, ensuring Microsoft technologies are properly leveraged to help solve specific needs.

Premier support provides access to proactive support services and the option to engage a Dedicated Support Engineer (DSE). Proactive support services will help defence organisations optimise their IT operations. Plus DSE provides an on-site resource with deep technical skill in specific product and/or IT domain area, which means specific individuals can be security cleared efficiently.



www.microsoft.com/asia/defence

Microsoft[®]