

A Dynamic Nucleus for Collective Cyber-Defence

Robert F Brammer, vice president and CTO of Northrop Grumman Information Systems, outlines the capabilities of the UK's new Federated Cyber Range

The 2011 security mission has a critically important cyber dimension that is growing dramatically. The increased threat and associated costs cut across all aspects of our national activity, and recently prompted Iain Lobban, director of GCHQ, to state, "I don't want you to take away the impression that it is solely a national security or defence issue. It goes to the heart of our economic well-being and national interest."

During the past few years, we have seen significant incidents involving cyber espionage by some national intelligence organisations (known as the Advanced Persistent Threat); cyber-crime, involving large-scale theft of money and intellectual property; and cyber-warfare, such as the attacks on the Republic of Georgia in 2008. A recent survey of these and related cyber-security developments gives further information and references. Whether targeted at defence, intelligence, government, commercial or the domestic sector, cyber-attacks are a threat to us all, and a successful defence will rely on a coherent and collective response based on advanced research and development (R&D).

Currently one of the largest providers of security capability to the US government, Northrop Grumman has created a Federated Cyber Range (FCR) using the latest generation technology at our Fareham facility in the UK. Opened in October 2010 by Gerald Howarth MP, Minister for International Security Strategy at the MoD, and capable of being networked with other cyber facilities, the FCR is the first commercially available cyber range in the UK.

It will initially be used in collaboration with Northrop Grumman's SATURN Partners (BT, Oxford and Warwick Universities and Imperial College London) to conduct a series of experiments, with the aim of improving the resilience of the UK critical national infrastructure. The SATURN Programme is part-funded by the UK government-backed Technology Strategy Board, the



The Federated Cyber Range includes advanced computing hardware and specialised technology and software to aid in developing cyber-security defences

Engineering and Physical Sciences Research Council and the Centre for the Protection of National Infrastructure.

The FCR looks similar to an enterprise data centre. However, it has special hardware and software that enable the key capabilities of a cyber range, and there are things you can test on the FCR that you would never replicate on any operational system. The FCR is a safe environment for simulating cyber-attacks and defences and for evaluating the security of various systems and networks. These four areas include common uses of the FCR:

- architecture evaluations
- component tests
- R&D
- training

The FCR is like a flight simulator in which pilots experience the same look and feel as a real aircraft. Pilots go through a series of well-defined scenarios, allowing them to respond to all kinds of malfunctions and flying conditions. This is a safe and controlled environment. The plane doesn't crash, no one is hurt, and the airlines don't lose money.

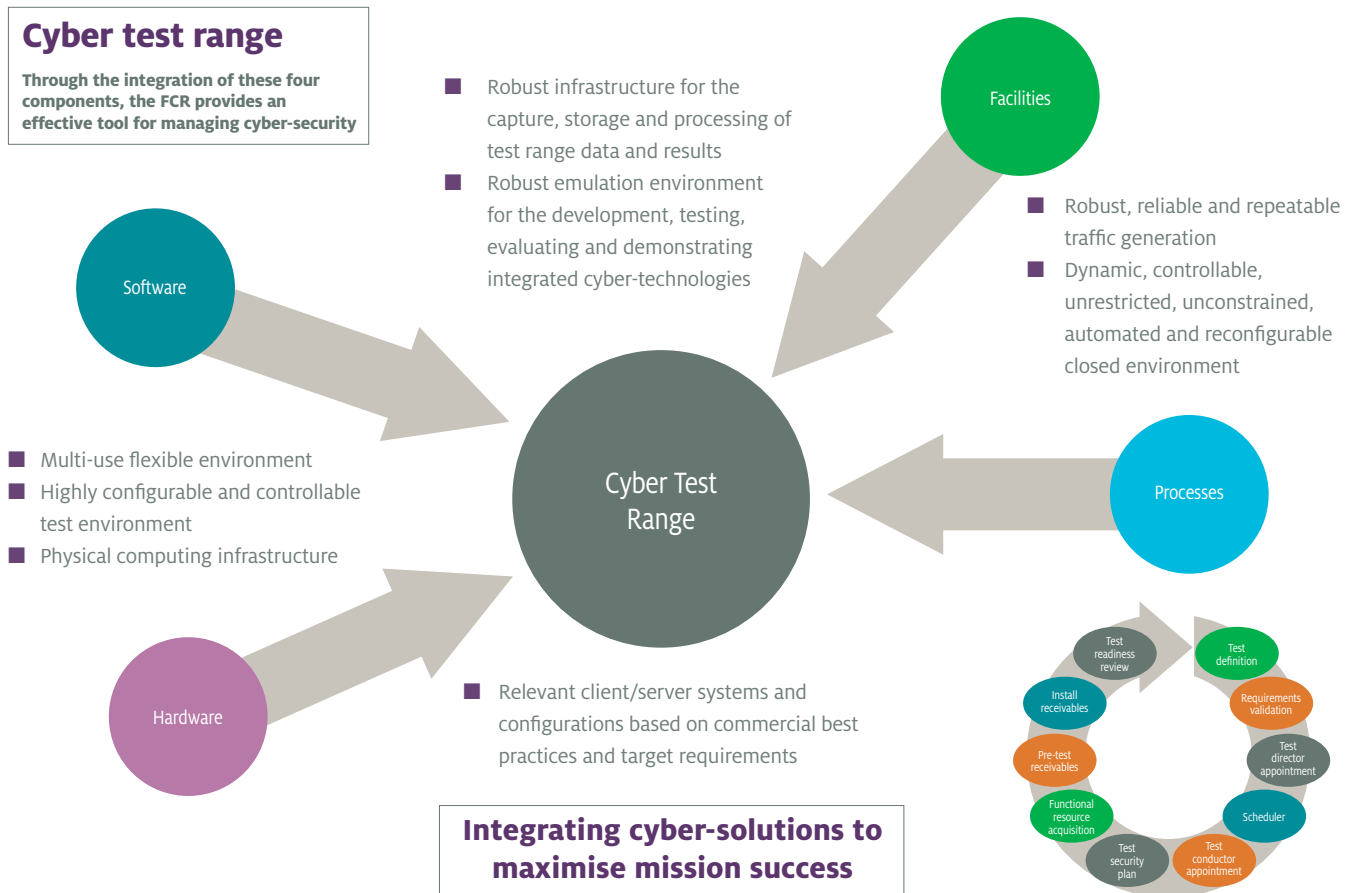
The FCR is very similar and provides logical 'virtual' models of a wide variety of computer and critical infrastructure networks. These models look and feel just like the real thing, with virtual users, departments, sites and representative operations. Simulating viruses, espionage strategies and cyber attacks in this environment provides response training for operators and decision makers. FCR controllers can stop the test at any time, reset it and start afresh with a clean system without having to worry about the malware, viruses and trojans unleashed earlier.

The FCR can also be a 'virtual wind tunnel' to test network designs for cyber-defence performance. Positioning a new asset in the network requires testing and tuning to optimise performance and minimise risk. From complete 'green-field' design opportunities to planning mass refreshes, upgrades, policies, processes and procedural creation, and employee testing and training, the FCR is a versatile and efficient tool to test design concepts.

Architectural evaluation

When attacked, a network may react in ways that lead to hitherto unknown behaviour, including cascade effects. The FCR is able to stress network designs in ways not advisable in an operational system. It enables analysis without disruption to the organisation's operation. For example, such testing could analyse the impact of proposed software changes to a network – or could analyse new system architectures before purchase. The FCR can model a variety of networks and operations, including infrastructure networks such as power grids and transportation networks in addition to enterprise computer networks.

Furthermore, it can test the resilience of security policies and their effect on operations. Applying a new security policy on a live network carries a high risk of causing serious disruption to operations, with subsequent loss



of revenue and the risk of alienating users/customers with unintended side effects. A recent study has shown that some employees may knowingly violate their organisation's security in order to expedite their work. The FCR can show the employees some implications of policy violations.

Test-driving and optimising a new policy in the FCR on a model of the organisation's network helps lead to an efficient and lower-risk roll-out. Northrop Grumman made use of our own range capabilities to model a roll-out of a new anti-malware system to our 120,000-seat global network. This helped in leading to successful implementation over a period of a few days in June 2010.

We can also test the architecture of various cyber-attack and defence strategies. Determining the effectiveness of defences against various types of threat is increasingly critical to organisational operations and assets. The FCR is also a perfect platform for testing network components, including new hardware and software products. Many companies are interested in having our staff members include their products in our tests, since the FCR can provide test environments for cyber-security threats that are not available elsewhere.

The FCR is an extremely versatile facility to support a wide range of research and development. Examples include the ability to develop tools to find and visualise potential vulnerabilities; develop countermeasures for new exploits/attacks; develop improved network protocols; or develop improved real-time methods of monitoring network health. We have developed a research agenda that includes many areas for FCR simulation and testing.

An organisation may not recognise that they are under cyber-attack, or react in time with the appropriate action. The FCR can be used to train network administrators to cope with unusual or hostile situations. This training can be grouped into two areas: prevention – designed to

reduce the likelihood of an organisation falling victim to a cyber-attack; and response – designed to improve the way in which an organisation handles a cyber-attack.

The FCR uniquely uses a high-fidelity model of an organisation's current or future proposed network that allows training to be immediately relevant, while removing any risk to the daily operation until the team has reached proficiency.

A range of benefits

The benefits of using the FCR are diverse. First, the FCR delivers confidence that the security status of critical networks is understood and the integrity of operations is safeguarded. Furthermore, testing and evaluation, using the system, helps to determine the best way forward in terms of trying before buying, identifying existing vulnerabilities, avoiding unnecessary technical churn and the associated financial bill, as well as planning the transition from a legacy system to the new system. The results of these tests are immediately transferable to the live operation on completion.

Additional benefits include the advantages of training in a safe environment – using adversarial training techniques to hone real-time defensive procedures in the knowledge that safety is being maintained, as well as the ability to practise techniques without disrupting a live network. Likewise, the FCR provides a platform for development of cyber-defence tools and the evaluation of their effectiveness. Moreover, the federated nature of the facility brings the advantages of scalability with the ability to bolt on additional ranges for specific projects.

Finally, another aspect which should not be overlooked is the technology and expertise reach back to the US. Northrop Grumman is, after all, one of the world's largest global security companies, and it operates its own global network and 7 x 24-hour cyber-security centre. ■