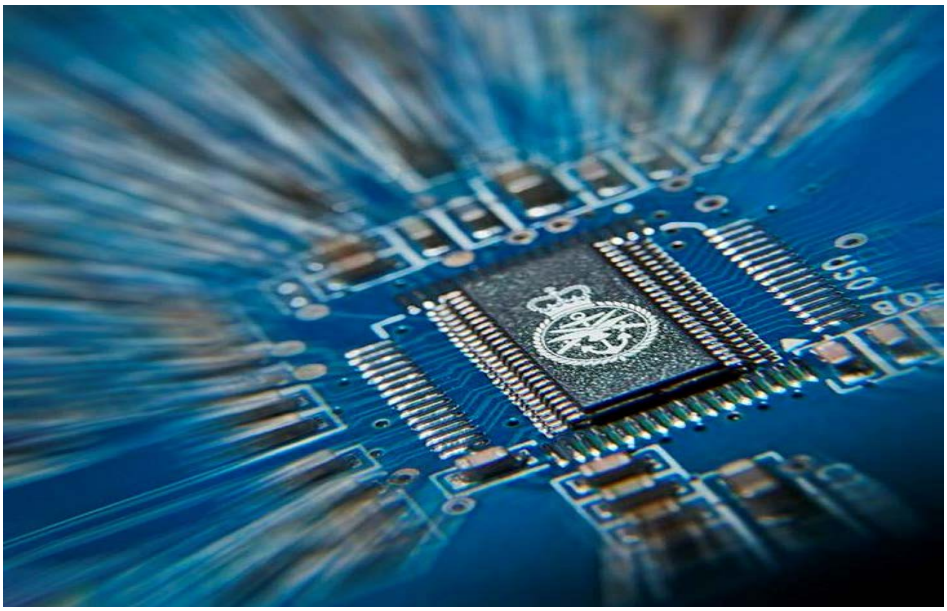
Centre for Defence Enterprise

CDE proves the value of novel, high-risk, high-potential-benefit research. We work with the broadest possible range of science and technology providers, including academia and small companies, to develop cost-effective capability advantage for UK armed forces and national security.

Automating cyber defence responses



This CDE themed competition seeks proof-of-concept research proposals for tools and techniques that support the planning and carrying out of automated responses to threats to our systems.

The total funding available for this competition is £1 million.

Competition networking event: Tuesday 9 September 2014 in London at De Vere Canary Wharf

Competition close: 23 October 2014 at 5pm

Crown Copyright (c) 2014 Ministry of Defence. Nothing herein shall be relied upon as constituting a contract, agreement or representation that any contract shall be offered in accordance herewith. MOD reserves the right, subject to the appropriate procurement regulations, to change without notice the basis of, or the procedures for, or to terminate the process at any time. Under no circumstances shall MOD incur any liability in respect thereof.

CDE: www.gov.uk/dstl/cde
Dstl: www.gov.uk/dstl

SBRI Government challenges. Ideas from business. Innovative solutions.

[dstl] Defence Science and Technology Laboratory

Ministry of Defence

Automating cyber defence responses

Background

Our armed forces rely on cyberspace to conduct successful operations and we must assume that adversaries seek to disrupt our systems.

Ministry of Defence (MOD) systems are complex, dynamic and often used in environments with unique threats. Once a system is compromised, a cyber attack can quickly escalate, so automated responses are an essential part of cyber defence processes. However, we must make sure that humans can still make decisions on defensive responses where appropriate.

An automated cyber defence response includes collecting information, identifying the attack, analysing potential courses of action and then responding.

In this CDE themed competition we seek proof-of-concept research proposals for tools and techniques that support the planning and carrying out of automated responses to threats to our systems.

Solutions must:

- consider both permanent infrastructure and deployed systems
- consider different responses, including allowing for human intervention
- identify defensive actions, processes and tactics to allow decisions to be made
- offer a significant improvement over the capability of current products and technologies

Successful bids will identify and justify where automation offers improvements in cyber defence, while recognising that the user may wish to revert to human decision making. Solutions must contribute to understanding what's happening and demonstrate how an appropriate course of action / cyber defence response has been selected.

We invite research proposals that draw from the widest possible range of emerging ideas and applications that could be used to automate Cyber Defence.

Up to £1 million is available for this themed competition.

Technology challenge: course of action tools

This competition seeks to address the need for an automated or semi-automated capability to change systems to dynamically respond to cyber events.

In response to operational demands, military networks and systems are becoming more complex and interconnected with other military systems, both internally and with allies, and also with commercial and civilian infrastructure. The military is relying more on information systems. Timely information sharing and cross-boundary information flows are critical to mission success. Similarly, attacks are becoming more sophisticated, distributed and stealthy, with potentially more damaging impact on military operations. This makes it more important, and more difficult, to identify, decide on and carry out timely cyber defence responses. Suitable responses will provide the best protection without hindering critical information flows and system availability to allow operations to continue unaffected.

An automated cyber defence response capability is made up of a number of functional elements working together to address the need. These functional elements include:

- collecting situational awareness data
- analysis to determine actual and possible attacks
- determining courses of action in response
- taking the appropriate actions

This CDE competition relates to the 'determining courses of action' element. We seek proposals for tools or toolsets that apply innovative approaches to support the determination, description and analysis of possible cyber defence courses of action.

Bidders should assume that the other elements listed above already exist as part of a cyber defence architecture, although their scope and interfaces may not be well defined and some overlap may exist. The course of action element will need to take input from and provide outputs to the other elements. A successful proposal will explain the nature of these interactions and the data required or provided by the solutions. It's anticipated that the successful developments will be used directly during pre-deployment and on operations to help decision making. They'll also be part of a course of action library which can be accessed as required to draw on previously defined courses of action.

There are a wide range of possible courses of action that need to be considered as responses to events. Relevant events could include but are not limited to:

- detected attacks or attack pre-cursors
- predictions from other sources of the change in likelihood or nature of future attacks
- indications of vulnerabilities in systems
- changes to the configuration of networks, systems or personnel

The responses required to such events might include but are not limited to:

- changing compartmentalisation and connectivity
- changing the configuration of security components such as firewalls
- controlling routing
- modifying systems' access controls and clampdown status
- managing service availability
- updating attack signature and patch levels
- warning staff or modifying staffing levels
- changing alert status levels
- tightening security operating procedures

Such responses may be undertaken individually or as a group. Responses may be to mitigate the effect of the detected events, decrease the likelihood of the success of an attack or future attacks, or contain the damage resulting from an attack. Solutions proposed should address and document a more exhaustive set of responses that will form the basis of identifying the course of action. Proposals should show how the tools and algorithms being developed can combine the responses into appropriate courses of action.

Each course of action must have a set of metrics (eg levels of risk, impact on missions) associated with it. The metrics should be designed to allow effective prioritisation of courses of action, comparison of one course of action with another, and to support decision making on whether actions should be taken automatically or manually. We expect proposals to list the types of metrics to be used, the benefits they provide and how they'll contribute to effective decision making. Solutions developed should then provide a more complete set with more detailed definitions of their meanings, value ranges and how they're used in deciding on possible courses of action and subsequent action decisions (both automated and with manual intervention).

Where an automated response is chosen, the course of action must be in a form where it could readily be interpreted by the military user. This response should give actionable commands to elements of the cyber defence architecture making use of appropriate standards (e.g. Simple Network Management Protocol for network management actions). The solution proposed must describe and demonstrate these different types of course of action output and show how translations to lower-level commands can be achieved. The output from the tools must also include descriptions of the courses of action considered and, where the course of action has been selected by the toolset, the course to be taken. This output could be used to populate a course of action library and would be used by a presentation service to aid human understanding.

In addition to a final report, we require a proof-of-concept demonstration to complete delivery of the contracted work.

What we want

Proposals must include:

- solutions leading to innovative or disruptive capabilities
- novel approaches to developing courses of action to secure information infrastructures
- practical proof-of concept demonstrations

An ideal proposal should include:

- a well-defined, clear and practical exploitation route
- consideration of systems and implementation issues
- solutions with standardised and adaptable interfaces to allow integration with other tools
- recommendations and proposals for further development

We anticipate that phase 1 proposals will be 6 – 9 months in duration. All proposals must be complete by March 2016.

What we don't want

Under this CDE themed competition we're not looking for:

- paper-based studies
- marginal improvements in capability
- solutions that offer no significant defence and security benefit
- technology watch or horizon scanning
- roadmaps or technology prediction
- demonstrations of existing technology products

Exploitation

Responses to this CDE competition must show that the solutions proposed have benefits that can be quantified and demonstrated. They must also describe well-thought-out and achievable exploitation routes, identifying necessary partners and the status of support from those partners.

Suppliers should note that Dstl won't provide data sets to support the development, testing or refinement of proposed projects. Suppliers must either supply their own or use relevant third-party data sets to demonstrate how their proposals are applicable.

Proposals will be assessed by subject matter experts from MOD and Dstl using the MOD Performance Assessment Framework.

Successful outputs of CDE funded projects from this themed competition may be taken forward under one or more of the defence science and technology research domains for phase 2 funding. Up to £1 million will be made available for this second phase and funding will be considered on a per-project basis.

Each project will be assigned a Technical Partner in Dstl who will provide the interface between the project and the defence and security community and will assist in developing potential routes to exploitation within the defence community if appropriate.

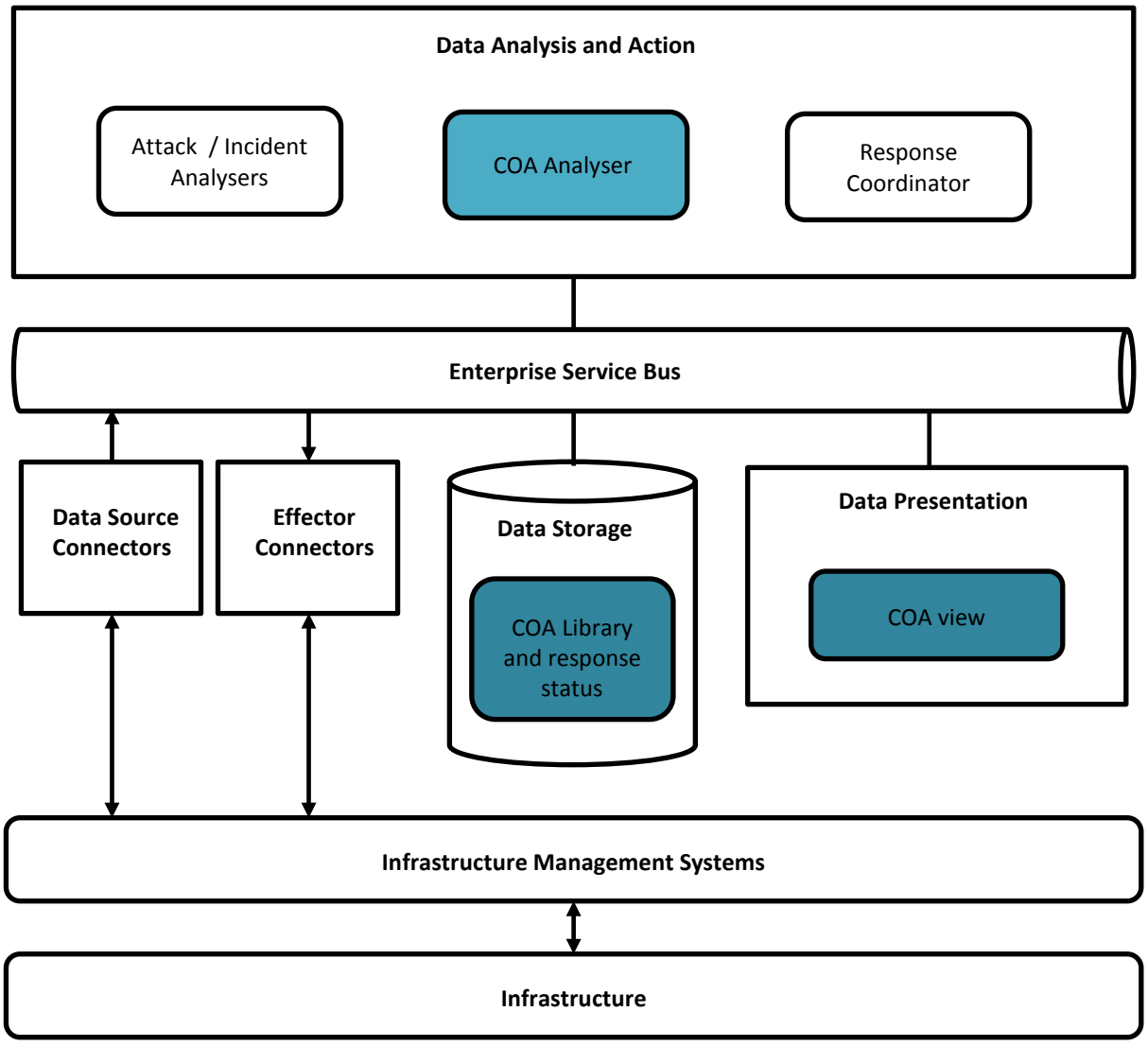
Deliverables from contracts will be made available to Technical Partners and subject to review by UK MOD.

Successful solutions may be integrated into an international collaboration (Australia, Canada, UK, US and New Zealand) on automated cyber defence response. This collaboration will be based around a Common Integration Framework (CIF) that will be used to explore, develop, and test new concepts of operation for dynamic defence and response to cyber-attacks. The CIF is already under development, although at this time the details of interfaces and standards used are not available.

Common Integration Framework Architecture

The CIF will be an open-source, standards-based Service-Oriented Architecture (SOA) approach, packaged and configured to allow distributed, decoupled integration of technologies, systems and data. It'll provide standardized interfaces, such that future components developed – eg sensor feeds, analysis engines, course-of-action algorithms, response mechanisms, and security metrics for decision making – will be compatible and work together. Successful outputs from this CDE competition must have the capability to interface to a SOA framework through an enterprise service bus (see below). Any further development work supported under phase 2 may require the solution to be integrated into the framework.

Figure 1: example high-level architecture showing example course of action (COA) components in a Service-Oriented Architecture (SOA) context



The example in figure 1 above uses a component-based approach. The responsibility for generating courses of action may be distributed among more than one tool or toolset.

Likely solutions will take input from multiple data sources, generating courses of action recommendations based on factors including, but not limited to:

- vulnerability risk metrics
- attack risk metrics
- exposure metrics
- operational implications
- network architecture
- patches and known mitigation strategies and techniques

Data analysis and action subsystem

This subsystem provides analysis of system information received as input from other components of the network and passes the results of analysis to the data storage and presentation subsystems.

Enterprise service bus

An open source enterprise service bus, based on the Apache ServiceMix container, provides the foundation of the SOA architecture enabling the integration of different components into a common framework.

Assumptions

- data will be processed and routed via the service bus
- data sources will include an array of network devices and management systems including:
    - firewalls, routers, intrusion prevention systems
    - vulnerability scanners
    - enterprise and network management systems
    - other, i.e. vulnerability assessments
- data may be pushed, scheduled or on demand

Important information

Proposals for funding must be submitted **by 5pm on 23 October 2014** using the CDE portal.
Please mark all proposals for this themed competition with **'Automating cyber defence responses'** as a prefix in the title.
Proposals will be assessed by subject matter experts from MOD and Dstl using the MOD Performance Assessment Framework (PAF).

Deliverables from contracts will be made available to Technical Partners and subject to review by UK MOD.

Technical queries should be sent to **cybersecuritycde@dstl.gov.uk**

General queries (including how to use the portal) should be sent **cde@dstl.gov.uk**

Invitation for CDE proposals

This competition will be supported by presentations given at the launch seminar on 9 September 2014. These will be available to download via the 'Automating cyber defence responses' competition page.

There is no cap on the value of proposals but it is more likely that at this stage a larger number of lower value proposals (ie up to £100,000) will be funded than a small number of higher value proposals.
Read important information on what all proposals must include on our website.

CDE proposal submission process

Key dates

- 9 September 2014 Competition launch event at *De Vere Canary Wharf, London*
- 18 September 2014 Post-launch webinar
- 23 October 2014 Competition closes at 5pm
- December 2014 Contract placement initiated and feedback provided
- March 2016 The latest date for the delivery of proof-of-concept research

Queries and help

As part of the proposal preparation process, queries and clarifications are welcomed:

- **Technical queries** about this specific competition should be sent to **cybersecuritycde@dstl.gov.uk** **Capacity to answer these queries is limited in terms of volume and scope. Queries should be limited to a few simple questions or if provided with a short (few paragraphs) description of your proposal, the technical team will provide, *without commitment or prejudice*, broad yes/no answers. This query facility is not to be used for extensive technical discussions, detailed review of proposals or supporting the iterative development of ideas. Whilst all reasonable efforts will be made to answer queries, CDE and Dstl reserve the right to impose management controls when higher than average volumes of queries or resource demands restrict fair access to all potential proposal submitters.**

- **General queries** (including how to use the portal) should be sent directly to CDE at **cde@dstl.gov.uk**

© Crown copyright *2014*.
Published with the permission of the Defence Science and Technology Laboratory on behalf of the Controller of HMSO.