Defence Research and Development Canada
Recherche et développement pour la défense Canada

C31 Group - Technical Panel 3 - Information Assurance and Cyber Defence

Technical Report: On the Boundaries of the Cyber Domain S&T

Peter C. Mason
Sean Stamplecoskie
DRDC Ottawa

Defence R&D Canada – Ottawa

Scientific Literature
DRDC Ottawa SL 2013-156
December 2013

Canada

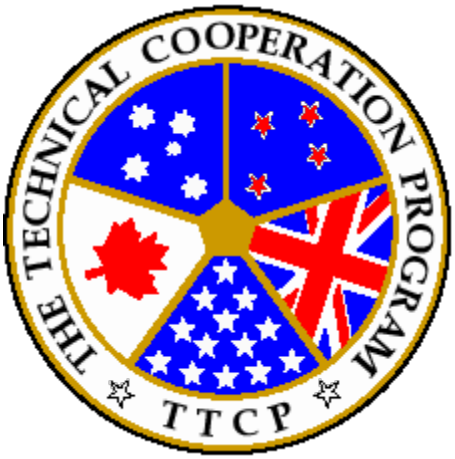
C31 Group - Technical Panel 3 - Information Assurance and Cyber Defence

Technical Report: On the Boundaries of the Cyber Domain S&T

Peter C. Mason
Sean Stamplecoskie
DRDC Ottawa

Defence Research and Development Canada – Ottawa

Scientific Literature
DRDC Ottawa SL 2013-156
December 2013



The Technical Cooperation Program

Australia - Canada - New Zealand - United Kingdom - United States of America

---

C3I GROUP – Technical Panel 3 – Information Assurance and Cyber Defence

Technical Report: On the Boundaries of Cyber Domain S&T

Peter C. Mason[1] and Sean Stamplecoskie[2]

[1]DRDC Ottawa, C31 TP-3 Canadian National Lead

[2]DRDC Ottawa EWS-TP-7 Canadian Representative

TR-C3I-TP3-1-2013
December 2013

This page intentionally left blank

Abstract

This report provides a series of scenarios that move progressively from what has been considered to be electronic warfare operations, finishing with those that are purely cyber operations. The intent is to demonstrate that the line between the two types of operations becomes blurred as coordination between the two separate domains is required to achieve an effects-based approach. This coordination will become increasingly important as militaries refine their Joint Targeting processes. The report then uses the scenarios presented to indicate where the boundary between the electromagnetic and cyber domains stands from the perspective of The Technical Coordination Program's panel on Information Assurance and Cyber Defence.

Résumé

Le rapport présente une série de scénarios, allant progressivement des opérations de guerre électronique aux opérations du domaine purement cybernétique. L'objectif est de démontrer que la ligne entre les deux types d'opérations est floue lorsqu'il faut coordonner les deux domaines distincts pour avoir une approche basée sur les effets. Cette coordination gagnera en importance à mesure que les forces militaires préciseront leurs processus de ciblage interarmées. Dans le rapport, les scénarios présentés sont utilisés pour illustrer où se situe la frontière entre le domaine électromagnétique et celui de la cybernétique du point de vue du groupe d'experts du programme de coordination technique en ce qui a trait à l'assurance de l'information et à la cyberdéfense.

Purpose

This report is a position paper. Its purpose is to provide background and context in order to better coordinate TTCP collaboration in Cyber Domain S&T, particularly when Cyber Operations can influence, or be influenced by, operations originating in other domains. In particular, this report provides some perspective on the coordination of activities between the Cyber and Electromagnetic Spectrum domains. It presents a series of scenarios that contain aspects of Cyber Operations and Electromagnetic Spectrum Operations which are intended to help clarify where each TTCP defence S&T community sees the boundaries of their Cyber S&T mandate.

1 Background

Certain Cyber Operations activities are affected by, and influence, operations in other domains. To examine how best to coordinate S&T activities in the 5-eyes community, a *TTCP Workshop on the Topic of Cyber Research Collaboration* was held at Dstl Porton Down in July 2013. The meeting consisted of members of TTCP C3I, EWS, ISTAR, and JSA. It became apparent at the meeting that the distinction between Cyber Operations and Electromagnetic Spectrum Operations, in particular, required greater clarity.

Information sharing among 5-eyes nations is subject to different agreements and releasability conditions, depending on the nature and intent of the activity. Nations may not have a common perspective or approach in defining their activities, with certain types of Cyber activities, in particular, residing in different organisations with differing mandates, within each nation. This results in difficulties in the coordination and sharing of Cyber S&T among nations.

Input into this report has come from the pan-group *TTCP Workshop on the Topic of Cyber Research Collaboration*, along with subsequent discussions held during the EWS TP8 Workshop on Electronic Warfare Battle Management held at the Australian Embassy in Washington, November 2013, and the TTCP C3I TP3 annual business meeting at Dstl Porton Down in November 2013.

2 Introduction

The Electromagnetic Spectrum (EMS) is a physical environment (domain) upon which all other domains (Air, Maritime, Land, Space, and Cyber) depend. The Cyber environment also supports all the other operational environments and is a domain in which operations can be conducted independently to achieve objectives. The US military definition of Cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems and embedded processors and controllers."[1] The Cyber environment, therefore, consists of the digital portion of the much larger Information Domain, along with the technologies used to control and process its contents.

The idea that Cyber and EMS domains are converging as part of a continuum has been put forward in a number of fora. We take the view articulated in a recent Journal of Electronic Defence, which argues that domains by their nature cannot converge and therefore the EMS and Cyber Domains remain distinct. The human-created Cyber domain cannot converge with the natural EMS domain any more so than it can converge with the air, maritime, or space domains.[2]

Electronic Warfare (EW) defined, again using US terminology, as "any military action involving the use of electromagnetic energy and directed energy to control the electromagnetic spectrum or attack the enemy."[3] That is, it is a means of influencing the EMS environment in order to achieve desired effects designed to influence capabilities in (at least) one of the other environments. For example, disrupting a radar can influence operations in the air domain, while disrupting signalling in the space domain can influence C2 and ISR. Similarly, Cyber Operations are information technology-based means designed either to directly influence the Information Environment or the technologies used to control it, or to influence operations in one of the other domains.

The proliferation and increasing sophistication of wireless networking technologies has increased the Cyber domain's dependence on the electromagnetic spectrum. At the same time, platforms such as Software Defined Radio, designed primarily in support of wireless networking, can equally be used to have distributed, and coordinated, effects on the EMS. This dual use of technologies represents a technical convergence point for systems used in support of Cyber and EW operations. This convergence between the technologies that shape and affect these domains demonstrates the pressing need to integrate and coordinate operations in the two domains, rather than a convergence of the domains themselves.[4]

[1] Alexander, Lt. Gen. Keith, http://www.nsa.gov/public_info/speeches_testimonies/5may09_dir.shtml
[2] Knowles, John., "Why Two Domains are Better than One", Journal of Electronic Defence, May 2013.
[3] FM 3-36 "Electronic Warfare in Operations", http://usacac.army.mil/cac2/Repository/FM336/FM336.pdf
[4] Elder, Lt. Gen. Robert J., USAF (Ret.), "21st Century Electronic Warfare", IO Journal, August 2010.

3 Scenarios

We step through a series of scenarios, introducing a new capability, or level of sophistication, with each step, in order to demonstrate the need to coordinate operations in the Cyber and Electromagnetic Spectrum domains. It is more didactic to examine offensive scenarios, so we present those first. Only one defensive scenario is given.

Offensive Scenarios

Each of the following scenarios is based upon a system of distributed red (adversarial) nodes capable of sensing the EM spectrum transmitting EM energy to affect/influence blue (friendly) nodes in the same operating environment.

Scenario 1. The red nodes act independently to jam a blue node. The transmitted EM energy is not modulated in a way to purposely carry information.

Scenario 2. Introduce a network to enable smarter local decisions. The red nodes are linked (networked) and share their sensor information amongst one another. Each red node fuses the sensed information and decides whether or not to transmit (jam) based on some (common) algorithm. The EM energy is not modulated in any way to purposely carry information.

Scenario 3. Introduce coordination to enable cooperative effects. Sensed information is now centrally analysed and an optimal strategy is determined. Red nodes then receive instructions from the network on how to collectively jam a blue node, or alternatively, deny access to portions of the EMS for the purposes of forcing blue nodes to choose technologies, strategies, or protocols where greater red Cyber capabilities exist for exploiting the blue nodes.

Scenario 4. Introduce targeted jamming of traffic type. Networked red nodes are able to analyse and target specific types of traffic at the packet level which they can jam. For example, it can target VOIP packets. Or nodes, with knowledge of network management traffic protocols, can selectively jam a small subset of control traffic to cause a specific response (e.g. jamming control packets).

Scenario 5a) Introduce EW targeting of information content, such as specific bits within a frame. If the bits targeted are in the header, this scenario may be equivalent to scenario 4 since the entire frame may appear as noise to the receiving node. However, if we leave header information intact while corrupting the payload, frames received by a node will be processed by the stack (thus using time, energy, and processing resources) before being discarded once an integrity check is performed.

5b) Instead of using the EW capabilities of the red nodes to corrupt blue traffic, let the red nodes instead craft corrupted frames to perform various levels of Denial of Service (DoS) on the blue network. The corruption can be done to targeted portions of the frame as in part 5a.

Scenario 6a) Introduce targeting of algorithms used for network command and control. Add a dynamic spectrum access (DSA) capability to the communicating blue nodes. Now, with knowledge of the co-operative DSA algorithms, red nodes can transmit energy timed in such a way that the DSA algorithms either do not converge or reach decisions that result in significantly reduced network throughput.

6b) Now let the red nodes transmit legitimate frames rather than energy, so they can be mistaken as legitimate blue node frames. As in Scenario 5, these frames are processed by the network, now affecting the network and spectrum access decision making as well as consuming resources.

Scenario 7. Due to some known vulnerability in the blue node network, a specifically crafted waveform sent by the red nodes causes a buffer overload in a blue node or activation of a process in the blue system that disrupts the network and leaves it vulnerable to further manipulation, such as the remote (via the EMS) delivery of an information (Cyber) payload or activation of a Trojan on the host system.

Defensive Scenario:

Man-in-the-middle or **replay attack** in a wireless network. The relayed or replayed packets are indistinguishable from legitimate packets in the Cyber domain, and do not break the protocol, so the attack is not detectable using Cyber domain techniques. However, the attack requires accessing the EMS and therefore has a physical fingerprint. Detection of this fingerprint can be done by the nodes in the network through their ability to sense the EMS. Analysis of the sensed data renders the Cyber attack detectable.[5] This defensive scenario is an example of a Cyber defense informed by sensing the EMS, and demonstrates the benefits of integrating efforts between the two domains.

[5] Edwards, J.J. et al. "*Using Covert Timing Channels for Attack Detection in MANETs*", Proceedings of IEEE MilCom 2012.

4 Discussion

In the offensive scenarios presented above, the TTCP C3I TP3 position is that scenarios 1-4 fall within an EMS Operation with increasing level of coordination with Cyber Operations. Scenario 4 demonstrates EW attacks on specific Cyber services. Scenario 5 shows where the coordination between domains can be very effective – here changing the portion of the frame that is targeted can have far broader Cyber effects. Alternatively, if the goal is simply to degrade the network by a certain percentage, intelligent jamming of the payload of a small percentage of frames could have the same desired effect as corrupting the headers of a larger percentage. This would make the detection and localisation of the attacking emitters more difficult.

According to Canadian Armed Forces doctrine, scenario 5a) is an EMSO, as is the 5b) operation of emitting corrupted packets such that that they are not able to be processed in the Information Domain. The 5b) operation where the frame contents cannot be identified as corrupt without processing by the stack falls within the Cyber Operations realm. The DRDC S&T Cyber Program is pursuing R&D into both scenarios 5a) and 5b), in coordination with scientists who work primarily in the EMSO domain.

Similarly, Scenario 6a) is seen as being an EMS operation, while 6b) is a Cyber operation. Scenario 6a) and 6b) both demonstrate the need for tight coordination between the Cyber and EMS domains to produce the desired effects on modern networking technologies.

Scenario 7 is an example of the type of problem that many suggest demonstrates convergence between the Cyber and EMS domains with there being a continuum between the two. It is more accurately described as a Cyber Domain vulnerability exploited via the EMS environment -- a coordination between the domains. Similar variants exist entirely in the Cyber domain (eg, variations on the Port Knocking theme[6]), or via the Information Operations domain. For example, social engineering can induce a human to make a change, either intentional or inadvertently, to a Cyber system leaving it vulnerable to Cyber exploitation. However, few would then argue that humans or information operations are a continuum of the Cyber domain. To further illustrate this point, a recent article published in the open literature by researchers at Fraunhofer FKIE articulates an attack on Cyber Systems via the acoustic medium.[7] There is no suggestion that this implies that the air domain is converging with the Cyber domain.

[6] http://www.portknocking.org/

[7] Hanspach, M., and Goetz, M., "On Covert Acoustical Mesh Networks in Air", Journal of Communications, vol. 8, no. 11, pp. 758-767, 2013. doi: 10.12720/jcm.8.11.758-767

5 Conclusions

Military operations are increasingly reliant upon the Cyber domain. The security problems of the Cyber domain remain a significant and growing challenge and it is incumbent upon the Defence Cyber S&T community to remain focused upon them. However, as operations in other domains develop to the point where they can influence the Cyber domain, and vice versa, S&T efforts should be devoted to the development of technologies and techniques that allow for integrated effects across domains. Defending the Cyber domain from attack vectors originating in the other domains is becoming an increasingly salient problem.

The capabilities in the Cyber and EWS domains in particular are complementary yet distinct,[8] yet it is the interdependence of operations in these domains that seem to be the testing ground for both setting bounds upon the Cyber domain and demonstrating the strategic importance of applying S&T to provide solutions that interconnect the capabilities within each. The optimal way for the TTCP defence S&T community to coordinate their S&T programs and exchange technical information in these areas remains an open question. This report is intended to help define steps in doing so.

[8] Buckhout, Col Laurie M., "Electronic Warfare and Cyberspace Operations: Where is the Convergence?", IO Journal, May 2010.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Defence Research and Development Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC APRIL 2011

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

On the Boundaries of the Cyber Domain S&T

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Mason, P.C.; Stamplecoskie, S.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
December 2013	16	0

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientifc Literature

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence Research and Development Canada – Ottawa
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC Ottawa SL 2013-156	TR-C31-TP3-1-2013

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This report provides a series of scenarios that move progressively from what has been considered to be electronic warfare operations, finishing with those that are purely cyber operations. The intent is to demonstrate that the line between the two types of operations becomes blurred as coordination between the two separate domains is required to achieve an effects-based approach. This coordination will become increasingly important as militaries refine their Joint Targeting processes. The report then uses the scenarios presented to indicate where the boundary between the electromagnetic and cyber domains stands from the perspective of ; The Technical Coordination Program's panel on Information Assurance and Cyber Defence.

Le rapport présente une série de scénarios, allant progressivement des opérations de guerre électronique aux opérations du domaine purement cybernétique. L'objectif est de démontrer que la ligne entre les deux types d'opérations est floue lorsqu'il faut coordonner les deux domaines distincts pour avoir une approche basée sur les effets. Cette coordination gagnera en importance à mesure que les forces militaires préciseront leurs processus de ciblage interarmées. Dans le rapport, les scénarios présentés sont utilisés pour illustrer où se situe la frontière entre le domaine électromagnétique et celui de la cybernétique du point de vue du groupe d'experts du programme de coordination technique en ce qui a trait à l'assurance de l'information et à la cyberdéfense.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

electronic warfare operations; cyber operations; scenarios