

Canadian
Forces
College

Collège
des
Forces
Canadiennes



CYBER SECURITY IN CARICOM: A SEMANTIC ANALYSIS

Maj G. Sterling

JCSP 42

Exercise Solo Flight

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2016.

PCEMI 42

Exercice Solo Flight

Avertissement

Les opinions exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

© Sa Majesté la Reine du Chef du Canada, représentée par le ministre de la Défense nationale, 2016.

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 42 – PCEMI 42
2015 – 2016

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER SECURITY IN CARICOM: A SEMANTIC ANALYSIS

Maj G. Sterling

“This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence.”

Word Count: 5000

“La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale.”

Compte de mots: 5000

Abstract

This paper examines the Cyber environment from a Caribbean perspective and argues that the Military and Constabulary Forces of Caribbean Community (CARICOM) must deliver the Cyber Operations capabilities required to support the security of the Cyber infrastructure within the Caribbean Region. In evaluating CARICOM's Cyber security requirements semantic gap, a comprehensive overview of the Cyber environment is outlined, including a detailed discussion of terminology and jurisdictional issues, computer network operations, the threats, vulnerabilities, risks and trends relating to public infrastructure, the military and constabulary, businesses and individuals. In assessing the roles and responsibilities across the various Governments of CARICOM and their relevant departments, a historical perspective is given of the progress since the publishing of the 2013 CARICOM Crime and Security Strategy (CCSS). The slow start in establishing clear governance structures, developing policies and implementing effective proactive solutions to the Cyber threat within CARICOM Member States is also mentioned. Related to policy difficulties, the operational and criminal legal issues highlight the complexities and immaturity of understanding of the Cyber environment and its regulation. The CARICOM Implementation Agency for Crime and Security (IMPACS) role and mandate is could be expanded to make it a valuable and essential capability for CARICOM as a regional Computer Network Defence (CND), Computer Network Exploitation (CNE) and Computer Network Attack (CNA) capability. However, additional resources would be required to fully execute the new mandate of fostering the development of proactive Cyber Operations as required by the member states of CARICOM.

Table of Contents

CHAPTER I – INTRODUCTION	1
CHAPTER II – THE CYBER ENVIRONMENT	3
Terminology	3
Defining the Cyber Environment	3
Cyber Network Operations	5
Threats, Vulnerabilities and Risks	8
Trends	8
Critical Infrastructure	9
Classifications	11
Military and Constabulary Mandates and Missions	12
Corporations	13
Individuals	14
CHAPTER III – MEMBER STATE CNO RESPONSIBILITIES	15
Cooperative Security Strategy	15
CARICOM Cyber Security Initiatives after 2013	15
Proactive Security Proposal	16
Legal Ramifications	17
Responsibilities	18
CHAPTER IV – POTENTIAL CNO CONTRIBUTIONS TO MEET CCSS MISSIONS	20
CHAPTER V – A SEMANTIC STATE FRAMEWORK	21
Principals	21
Abstraction	21
Semantic State Governance Layer	24
CHAPTER VI – CONCLUSION	25
Bibliography	27
Appendix 1	i

CHAPTER I – INTRODUCTION

The Caribbean Community (CARICOM)¹ has one of the fastest rates of technology uptake in the world in 2014.² According to PwC’s Global State of Information Security Survey 2015, cited by David Jessop,³ this growth in the rate of diffusion of technology occurred amidst a 48 percent rise in cyber-attacks globally in the same year. He further argues that “the Caribbean remains woefully unprepared, with governments and parts of the private sector declining to take the matter seriously until subject to an attack.”⁴ This observation is supported by a distinct upturn in malicious attacks across the region over the last three years.

CARICOM is predominantly a trading bloc of English speaking countries within the Caribbean.⁵ Defence and security cooperation within the bloc has primarily been fostered through the efforts of nations outside of the Caribbean such as the United States of America (USA) through its Southern Command (SOUTHCOM).⁶ The eminent threat of cyber-attacks crystalizes the need for a more concerted effort to understand and secure this domain as a

¹ Caribbean Community Secretariat, “Revised Treaty of Chaguaramas Establishing The Caribbean Community including the CARICOM Single Market and Economy”, last accessed 5 May 2016.
https://issuu.com/caricomorg/docs/revised_treaty_text;

² Symantec Corporation, *Latin American and Caribbean Cyber Security Trends*, (Washington: OAS Press, 2014), 91 p.

³ David Jessop, “New Threats to Caribbean Cyber Security”, *View From Europe*, (August 2015):
https://www.google.ca/search?q=david+jessop+new+threats+to+caribbean+cyber+security&ie=utf-8&oe=utf-8&gws_rd=cr&ei=wb8xV4b5IaSCjwTrr7ngCg#q=david+jessop+new+threats+to+caribbean+cyber+security+view+from+europe;

⁴ Ibid.

⁵ Caribbean Community Secretariat, “Revised Treaty of Chaguaramas Establishing The Caribbean Community including the CARICOM Single Market and Economy”, last accessed 5 May 2016.
https://issuu.com/caricomorg/docs/revised_treaty_text;

⁶ Department of State. “Caribbean Basin Security Initiative,” last accessed 5 May 2016,
<http://www.state.gov/p/wha/rt/cbsi/>.

collective.⁷ Additionally, member states and external actors have recognized the urgency and have initiated activities aimed at securing national infrastructure.⁸ This fractured approach can best be described as duplicitous and inadequate.

Cyber Network Operations have been categorized in a number of military concepts and doctrinal literature; these speak to the effects to be created at the strategic, operational and tactical levels within the cyber environment. Therefore, this paper argues that CARICOM must deliver the cyber network operations capabilities required to support the CARICOM Crime and Security Strategy (CCSS)⁹ in the cyber environment. In support of this thesis, Chapter II, serves to situate CARICOM within the cyber environment. Chapter III addresses some of the governance, legal and jurisdictional issues associated with the conduct of cyber operations; highlighting the shared, multinational and multi-organizational nature of conducting cyber operations within CARICOM. Chapter IV looks at the possible roles of possible implementation agencies and Chapter V proposes a Semantic Framework¹⁰ for achieving the shared security. The paper then concludes that there must be a strong coordinated approach to regional cyber security.

⁷ Caribbean Community Secretariat, "Crime and Security Strategy" (Turkeyen: Guyana, 2013), 64 p.

⁸ Global Forum on Cyber Expertise. "OAS Cyber Security Initiative," last accessed 25 March 2016. <http://www.thegfce.com/initiatives/cyber-security-initiative-in-oas-member-states>.

⁹ Caribbean Community Secretariat, "Crime and Security Strategy" (Turkeyen: Guyana, 2013), 64 p.

¹⁰ Roberto Baldoni and Gregory Chockler. Collaborative Financial Infrastructure Protection. Springer, 2012.

CHAPTER II – THE CYBER ENVIRONMENT

Terminology

Communication and Information Technology (ICT) affected by military concepts are generally termed Communication and Information Systems (CIS).¹¹ CARICOM countries tend to adopt doctrine from NATO and its allies in drafting policies and developing cyber strategies. Though fairly mature, these doctrine do not all agree and the results are often dissonant from country to country. One such concept is that of Information Operations versus Influence Operations. The Defence Research and Development Centre (DRDC) suggested that the conceptual basis of Influence Operations is British with an American implementation.¹² The US doctrinal publications, CARICOM and member states' draft and ratified documentation and the Concise Oxford dictionary¹³ will be used for cyber definitions within this paper.

This paper will utilize the more focused definition of cyber relating strictly to computers or computer networks.¹⁴ The Concise Oxford also offers the definition of the term environment as being “the overall structure within which a user, computer, or program operates.”¹⁵ The combination of these two definitions will be used to represent the cyber environment throughout this paper.

Defining the Cyber Environment

¹¹ NATO AAP-6 defines CIS as a collective term for communication systems and information systems.

¹² Keith Stewart. DRDC Toronto. “Influence Operations: Historical and Contemporary Dimensions”, DRDC Toronto CR-2007-126, 31 July 2007, last accessed 15 April 2016, <http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf>

¹³ The Concise Oxford Dictionary is the primary source of terminology for CARICOM whenever there is no Member State agreed term.

¹⁴ Concise Oxford Dictionary Online. Last accessed 30 March 2016 http://www.askoxford.com/concise_oed/cyber?view=uk; Definition of Cyber: combining form relating to information technology, the Internet, and virtual reality: cyberspace.

¹⁵ Concise Oxford Dictionary Online. Last accessed 30 March 2016 http://www.askoxford.com/concise_oed/environment?view=uk; Definition of Environment.

With the definition of cyber environment in the previous section, this section will attempt to characterize its peculiarities to CARICOM. Within member states there needs to be an agreed conceptual framework for the cyber environment that separates it from the established Land, Air and Maritime environments and considers it as more than an enabler to those environments. Additionally, the cyber environment should not be confused with the virtual environment.¹⁶ The distinction is necessary to facilitate classification of the nature of the cyber environment and appreciate types of attacks and influence therein. There is also the jurisdictional, national and internal organizational resistance to newly introduced concepts.

According to US Airforce Commander, General Kevin Chilton, the cyber domain "...is a warfighting domain everyone needs to understand..."¹⁷ Conversely, within CARICOM, cyber incidents are seen as primarily criminal acts and the move to warfighting may be considered a quantum leap. The CARICOM Crime and Security Strategy (CCSS) described such events as cybercrimes.¹⁸ The US term cyberspace will be synonymous with the term cyber environment as used within this paper. However, one potential pitfall in the US' approach is that it sees "...information operations in terms of ...the domination of cyberspace",¹⁹ though that possibility is still debatable. And, in taking the convergence of available technologies, such as the electromagnetic spectrum and electronics, into consideration the implications for existing and

¹⁶ Merriam-Webster Dictionary Online. Last accessed 15 February 2016. <http://www.merriam-webster.com/dictionary/virtual>; Defines Virtual as: being on or simulated on a computer or computer network.

¹⁷ Sean Gallagher, "The Right Stuff for Cyber Warfare", *Defense Systems*, (20 October 2008). Last accessed 16 February 2016. <http://defensesystems.com/Articles/2008/10/The-right-stuff-for-cyber-warfare.aspx>; A Defense Systems interview with General Chilton.

¹⁸ Caribbean Community Secretariat, "Crime and Security Strategy" (Turkeyen: Guyana, 2013), 64 p.

¹⁹ Keith Stewart. DRDC Toronto. "Influence Operations: Historical and Contemporary Dimensions", DRDC Toronto CR-2007-126, 31 July 2007. Last accessed 15 April 2016. <http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf>.

planned organizations, authorities, jurisdiction and policies and further research would be required to ascertain if CARICOM should proceed similarly.²⁰

Cyber Network Operations

In attempting to place Cyber network operations (CNO) in the context of CARICOM it is important to note that there is no established definitions within the community or the wider OAS. Therefore for this paper the CF definition "...actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting (fully utilizing) and protecting one's own information."²¹ will be adopted. However, the discussion should not be entirely military and CARICOM should seek to distill the core intellectual nuggets within information operations and influence operations as argued by LeBlanc and Knight:

While originally conceived in a military context, information operations are equally relevant to the new global threat environment and can find application in critical infrastructure protection, counter-intelligence, and contending with organized criminal activity.²²

Thus, proceeding with the assumption that irrespective of the outcome of the IO debate, CARICOM needs to develop certain cyber operational capabilities. The concept of CNOs speaks to the creation of tactical, operational and strategic effects within the cyber environment. These effects should be in response to emerging technology and the evolving use thereof by both

²⁰ David Jessop, "New Threats to Caribbean Cyber Security", View From Europe, (August 2015): https://www.google.ca/search?q=david+jessop+new+threats+to+caribbean+cyber+security&ie=utf-8&oe=utf-8&gws_rd=cr&ei=wb8xV4b5IaSCjwTrr7ngCg#q=david+jessop+new+threats+to+caribbean+cyber+security+view+from+europe.

²¹ Department of National Defence. B-GG-005-004/AF-010, *CF Information Operations*, (Ottawa: DND Canada, 1998-04-15), 1-2.

²² Sylvain Leblanc, Scott Knight, "Engaging the Adversary as a Viable Response to Network Intrusion", Workshop on Cyber Infrastructure Emergency Preparedness Aspects, Ottawa, 21-22 April 2005; last accessed 20 February 2016 <http://tarpit.rmc.ca/knight/papers/IO%20Counter-measures.doc>.

friends and enemies. The current CARICOM threat environment is focused on cybercrime,²³ but this paper argues that it would be imprudent to continue to delay consideration of the politico-military aspects of cybersecurity indefinitely.²⁴

Though the concept of IO in CARICOM is new²⁵ one realization among member states should be that Computer Network Operation (CNO) is a key enabler of IO.²⁶ Thus the journey from protection to militarization of cyber infrastructure should begin as it will only aid CARICOM's understanding of the role and purpose of CNO.²⁷ While not considered by this paper, the term Computer Network Warfare (CNW)²⁸, which leverages the tried and tested electronic warfare body of knowledge, has also been used to help add clarity to the concept of militarizing the cyber environment.

Individual member states have been embarking on the development of cyber security strategies, however, as a regional body CARICOM has not been able to coordinate the efforts in

²³ Caribbean Community Secretariat, "Crime and Security Strategy" (Turkeyen: Guyana, 2013), 64 p.

²⁴ Jose de Arimateia da Cruz and Taylor Alvarez, "Small Islands, Big Problems: Cybersecurity in the Caribbean Realm", *Small Wars Journal*, (December 2015). Last accessed 20 April 2016
<http://www.smallwarsjournal.com/printpdf/34462>.

²⁵ Neil Chuka, "Confusion and Disagreement: The Information Operations Doctrine of the US, the US, AUS, CA and NATO", (Master's Thesis, Royal Military College of Canada, 2007), 8. See Neil Chuka's dissertation for a full discussion on Info Ops, which he defines as "not foremost about technology or disrupting the ability of an adversary to conduct operations; at their most basic, Info Ops, as a coordinating and integrating function, are about conceiving and synchronizing activities, both physical and psychological, to create desired effects that influence the perceptions of the target audience and affect behaviour in a desired manner."

²⁶ *Ibid.*, 2.

²⁷ Ron Smith and Scott Knight, "Applying Electronic Warfare Solutions to Network Security", *Canadian Military Journal*, Vol. 6, No. 3, (Autumn 2005). Last accessed 20 February 2016.
<http://tarpit.rmc.ca/knight/papers/Applying%20Electronic%20Warfare%20Solutions%20to%20Network%20Security%20-%206%20Apr04.doc>;

²⁸ *Ibid.*, 1.

this regard.²⁹ Thus, outside of the cybercrime realm there is no commonality in approach by member states. Consequently, this paper uses the CF CNO Policy definition in continuing to frame the discussion.³⁰ CNO can be further dissected into Computer Network Defence (CND)³¹, Computer Network Exploitation (CNE)³² and Computer Network Attack (CNA).³³

In keeping with convergence of technologies it is suggested that the definitions of CNO, CND, CNE and CAN be expanded to include all aspects of the cyber environment and not just computer networks. Thus individual and SCADA devices would need to be considered in any common lexicon developed going forward.³⁴ As the arguments continue to be made for improved cyber capabilities, the matter of dealing with threats, vulnerabilities and risks are now considered.

²⁹ David Jessop, “New Threats to Caribbean Cyber Security”, View From Europe, (August 2015): https://www.google.ca/search?q=david+jessop+new+threats+to+caribbean+cyber+security&ie=utf-8&oe=utf-8&gws_rd=cr&ei=wb8xV4b5IaSCjwTrr7ngCg#q=david+jessop+new+threats+to+caribbean+cyber+security+view+from+europe.

³⁰ Draft CNO Policy, 22 Apr 08 version. Attached to the CNO definition is the following Note: To ensure clarity and precision, the phrase Computer Network Operations (CNO) shall not be applied to any single subordinate CNO discipline (i.e. - to CND, CNE, and / or CNA). Rather, the phrase shall only be used to describe activities involving two or more of the subordinate CNO disciplines. When an activity falls exclusively within the scope of a particular discipline (i.e. CND, CNE, or CNA), the appropriate phrase shall be employed.

³¹ Ibid. (Draft CNO Policy, 22 Apr 08 version.) Attached to the CND definition is the following Note: Any and all computer network activity, including a CND activity, that initiates intrusive contact (transcending the level of contact available on a public access basis) with other computers or computer networks, without the permission of the owner / operator of those computers or computer networks, constitutes CNE or CNA, depending upon the form of the contact, and falls under the governance framework of the corresponding activity.

³² Ibid.

³³ Ibid.

³⁴ Increasingly, multi-function devices such as cellular telephones and audio players contain flash drives and small, high-storage hard drives that enable the easy portability of large amounts of data. The result is an expansion of the network endpoint, since unauthorized devices can be connected to enterprise systems and authorized devices can be connected to unauthorized systems and networks. This has resulted in an increased attack surface and a higher number of potentially viable entry points for malicious code and attacks. A recent survey has suggested that over 43 percent of enterprises have little or no measures in place to address permissions or restrictions on removable media within their networks. Moreover, less than 17 percent use endpoint security measures to address the issue.⁴⁰ With increases in data theft and data leakage, these devices represent a viable attack vector for attackers as they attempt to steal as much information from as many sources as possible.

Threats, Vulnerabilities and Risks

The nature of cyber events today points to an ever present threat within the cyber environment. Taking the classic definition of threat “Threat = capability + intent” one has to be careful not to sensationalize the plethora potentially devastating outcomes in looking at the cyber threats. Thus, in order to focus the efforts of individuals, businesses and governments attempts have to be made to identify the possible attackers and associated intent prior to a cyber event.³⁵ By considering what vulnerabilities exist within the environment³⁶ and categorizing both the threats and the vulnerabilities the risks can be better assessed. Solce goes further to describe the attack vectors as cyber weapons putting them into two broad categories: semantic and syntactic.³⁷ Though both types of event can occur in a single episode, the physical elements must also be considered.³⁸ As was shown in the cyber events in Estonia in 2007 targeting individuals and corporations can have devastating effects if well-coordinated.³⁹

Trends

Symantec’s 2014 Latin American and Caribbean Cyber Security Trends Report showed five major trends in 2013 that were expected to grow into the future.⁴⁰ These trends are briefly explored for better understanding. Though the paper does not do an in-depth analysis it is important to list them here: (i) data breaches are on the rise; the target of cybercrime and

³⁵ Symantec Internet Security Threat Report Trends for July–December 07, Volume XIII, Published April 2008, 30.

³⁶ Bell Canada. “Carrier Grade Threat and Vulnerability Intelligence”, December 2008, 1.

³⁷ Natasha Solce, “The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force”. *Albany Law Journal of Science and Technology*. #18 (2008), 305.

³⁸ Martin C. Libicki and Rand Corporation, “Conquest in Cyberspace : National Security and Information Warfare” (Cambridge: Cambridge University Press, 2007), 8.

³⁹ Jason Richards, “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security”, *International Affairs Review*; last accessed 25 March 2016 <http://www.iar-gwu.org/node/65.html>.

⁴⁰ Symantec Corporation, Latin American and Caribbean Cyber Security Trends, (Washington: OAS Press, 2014) 91 p.

hacktivism, more than 552 million identities were exposed in 2013. 32 percent of breaches was accounted for by hackers⁴¹, (ii) Targeted attacks continue to grow; these attacks are evolving and becoming stealthier through additions such as watering-hole attacks to existing spear-phishing toolkits.⁴², (iii) Social media scams are on the rise; cybercriminals exploited the increased interconnectivity of social media sites and the resultant increased online sharing of information.⁴³, (iv) Banking Trojans and heists; many financial institutions have been compromised but there is significant underreporting.⁴⁴, (v) Major events provide rich targets; events such as the 2007 World Cup of Cricket in the Caribbean and the 2014 Football World Cup in Brazil were lucrative targets for malware operations, phishing schemes, and email scams.⁴⁵

Critical Infrastructure

The OAS lists the critical infrastructure pertinent to CARICOM as being the energy, telecommunications, water supply, transport, finance, health, and other infrastructures that allow a nation to function.⁴⁶ These are not unique to the Caribbean but the varying degrees of automation, within a region with the fastest rate of diffusion of technology in the world,⁴⁷ present some unique challenges. Therefore, the three basic trends affecting infrastructure and their

⁴¹ Symantec Corporation, Latin American and Caribbean Cyber Security Trends, (Washington: OAS Press, 2014), p 27.

⁴² Ibid.

⁴³ Ibid.

⁴⁴ Ibid.

⁴⁵ Ibid.

⁴⁶ Peter Burnet, "The Vital Role of Critical Information Infrastructure Protection (CIIP) in Cybersecurity", Report on Cybersecurity and Critical Infrastructure in the Americas, (Trend Microsystems and OAS), 2015. p 13.

⁴⁷ Symantec Corporation, Latin American and Caribbean Cyber Security Trends, (Washington: OAS Press, 2014), p 27.

associated risks and vulnerabilities make cyber threats more imminent for some states when compared to others.⁴⁸ Additionally, the absence of, or poorly managed, public-private partnerships (PPP) in member states where large sectors of the infrastructure continuum is owned and or operated by private corporations, the threat management is often weak.⁴⁹ The attendant issues are further compounded by the permeation of interconnectedness through the physical, organizational, procedural and informational layers.⁵⁰ These levels of interconnectedness also affects the response to failure, whether intentional or accidental, as different resources are required to counter each.⁵¹

The most visible government departments and utility companies are the most dependent on ICT, particularly in times of crisis. Within CARICOM the militaries and constabularies are mandated to assist in times of disaster.⁵² Additionally, much of the modern communication, including mobile services, rely on commercial links and platforms. However, care should be taken by the CARICOM Implementation Agency for Crime and Security (CARIMPACS)⁵³ and

⁴⁸ Myriam Dunn Cavelt, *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age* (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 18.

⁴⁹ Peter Burnet, “The Vital Role of Critical Information Infrastructure Protection (CIIP) in Cybersecurity”, Report on Cybersecurity and Critical Infrastructure in the Americas, (Trend Microsystems and OAS), 2015. p 14.

⁵⁰ The physical linkages between information systems is easily appreciated, particularly when the Internet provides connectivity to infrastructure control systems as well as administrative computer networks. What is less obvious are the informational and contextual relationships and interdependencies across systems. For example, the organizational and procedural regulations and practices between utility companies from province to province or even cross-border with the US. If one company programs its distribution network to divert overflow electricity to another company’s network, this has to be done through common, agreed-to procedures.

⁵¹ Myriam Dunn Cavelt, *Cyber-Security and Threat Politics : US Efforts to Secure the Information Age* (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 20.

⁵² Jamaica Defence Force, *Jamaica Defence Force Tasks*. Last Accessed 23 March 2016, <http://www.jdfmil.org/jdfTask/tasks.php>.

⁵³ Caribbean Community Secretariat, “Crime and Security Strategy” (Turkeyen: Guyana, 2013), 64 p.

local authorities to guard against the technologies offered by the companies and the use of leading edge technologies similar to how other militaries within the Americas operate.⁵⁴

This speaks to the need for militaries and constabularies to develop strategies with industry to meet their peak demands. This would create efficiencies that benefit all users of ICT. An attendant challenge is for governments to be knowledgeable enough about solutions implemented by industry that realistically indicate the levels of exposure of critical infrastructure at the physical, semantic and syntactic layers of the cyber environment.

Classification

Another reality regarding threats is the classification under which they fall. This shrouds vulnerability information and prevents a better understanding among a larger audience. Persons who need to be, are aware and, are entrusted with the details of breaches, attacks, vulnerabilities and other Cyber-events; not the general public. These reasons, ranging from national security concerns to business survival and profit, create dilemmas for Cyber security practitioners regarding allocation of resources for Cyber security when incidents are rarely exposed.

There may be little to redress this situation and certainly, for governments and their departments, secrecy surrounding threat levels and the vulnerability to these threats are likely to remain classified or on a need-to-know basis, but with the right reporting mechanisms, the decision makers can be briefed accordingly. CARICOM arguably possess these mechanisms but the

⁵⁴ DoD Instruction 8100.3, Department of Defense Voice Networks. Last accessed 16 April 2016 <http://www.dtic.mil/whs/directives/corres/pdf/810003p.pdf>. The CF operates in the harshest, most austere and extreme scenarios where mission failure is not an option. To coordinate such a large and geographically dispersed organization as the CF requires fail-safe ICT services. DND also operates an extension of two US voice networks, the Defense Services Network (DSN) and the Defense Red Switch Network (DRSN) in Canada and under the MOU agreement with DISA Last accessed 16 April 2016, <http://www.state.gov/documents/organization/111449.pdf> ; DND must comply with policies and interoperability standards of this network. Rigorous testing is performed on all equipment connected to these networks in accordance with DISA Information Assurance Test Plans, Last accessed 16 April 2016 [http://www.disa.mil/dsn/webfiles/DISA_Information_Assurance_Test_Plan_\(IATP\)v3_1March_2005.pdf](http://www.disa.mil/dsn/webfiles/DISA_Information_Assurance_Test_Plan_(IATP)v3_1March_2005.pdf).

divisions of responsibility are just being explored. This paper cannot discuss classified matters but will seek to ventilate matters not so classified.

Military and Constabulary Mandates and Missions

Militaries in CARICOM member states cooperate primarily as a corollary to other provisions of the Treaty.⁵⁵ Consequently, there are no bilateral agreements between member states. However, there are agreements with other states such as the US and Canada.⁵⁶ Conversely, the constabularies have greater levels of cooperation based on their primary crime fighting role. Both use commercial means of communication extensively and vulnerabilities either with service providers or other partners could easily be a source of compromise. This point is even more critical given the reliance of CARICOM defence and security apparatuses on foreign assistance⁵⁷ and the perception of weakness within the chain could mean no information sharing with those entities. One possible way of countering such eventuality is disclosing all of the security and communications requirements to prospective bidders for contract provision. This would mean greater levels of security screening for employees and companies. Also greater responsibility would be on businesses to protect sensitive and classified information stores and infrastructure.

⁵⁵ Caribbean Community Secretariat, “Revised Treaty of Chaguaramas Establishing The Caribbean Community including the CARICOM Single Market and Economy”, Last accessed 5 May 2016. https://issuu.com/caricomorg/docs/revised_treaty_text.

⁵⁶ Canada. Bilateral agreements between Jamaica and Canada are often the way much needed resources are accessed. Last accessed 24 April 2016. <http://www.forces.gc.ca/en/news/article.page?doc=strengthening-the-core-of-the-jamaica-defence-force/ht17dcd>;

⁵⁷ Ibid.

The singular question to be answered for CARICOM is the point at which a cyber event ceases to be a criminal matter and become an act of violation of a nation's sovereignty.⁵⁸ Thus the militaries may have different requirements for screening and disclosure when dealing with businesses and other military partners.

Corporations

Even reputable companies can become victims of internal or external cyber events. It becomes more critical to a nation's interests when those companies are custodes of sensitive or classified data and infrastructure.⁵⁹ While corporations have a responsibility to provide protection of their critical information infrastructure (CII) governments have a responsibility to ensure survivability and continuity either through direct involvement or the creation and enforcement of legislation. One key partner in this respect is the internet service provider (ISP) who is sometimes uniquely positioned to help.⁶⁰ Many such corporations within CARICOM are subsidiaries of multinationals and so normally have robust continuity plans. Local companies are not at the same levels of preparedness within many of the member states.

Thus it can be argued that graduate level collaborations with the region's universities, or even farther afield, could help in bridging the existing gap. Additionally, leveraging PPPs can help to create synergies similar to those in the more developed countries such as the Defence Advanced Research Projects Agency (DARPA) Trust in Integrated Circuits Program.⁶¹

⁵⁸ Jose de Arimateia da Cruz and Taylor Alvarez, "Small Islands, Big Problems: Cybersecurity in the Caribbean Realm", *Small Wars Journal*, (December 2015), last accessed 20 April 2016. <http://www.smallwarsjournal.com/printpdf/34462>.

⁵⁹ <http://www.eimagazine.com/xq/asp/sid.0/articleid.5CE830BB-4E47-4488-A245-90A8E4140C69/qx/display.htm>; Last accessed 16 April 2016.

⁶⁰ Bell Canada. Carrier Grade Threat and Vulnerability Intelligence, December 2008, 1.

⁶¹ Sally Adey, "The Hunt For The Kill Switch", *Spectrum IEEE*, Vol. 45, Issue 5, (May 2008). Last accessed 8 April 2016. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4505310;

Individuals

One of the lessons learned from the Estonian attacks is that harnessing the power of large numbers of personal computers can facilitate devastating cyber events. Thus increasing the awareness and voluntary compliance in protecting individual devices must be a priority of governments and businesses alike.

Also, tapping into projects like the World Community Grid (WCG)⁶² can help to boost the available computing power for defence, security or research without additional costs to the government.

⁶² World Community Grid, <http://www.worldcommunitygrid.org/> ; Internet; accessed 2 March 2009.

CHAPTER III – CARICOM CNO RESPONSIBILITIES

Cooperative Security Strategy

CARICOM's IT security has been the purview of the individual member states.⁶³ To date only four countries have developed or promulgated cyber security strategies.⁶⁴ However, as a region, CARICOM has not sought to develop cyber capabilities beyond fighting cybercrimes.⁶⁵ Jamaica's Cyber Security Strategy of 2014 showed a growing awareness of the reliance of the public and private sectors on the ICT for the provision of services amidst the rapid evolution of cyber threats.⁶⁶ However, while the strategy spoke to the prevention, detection, response and recovery from attacks on CII it was found to imprecise. Trinidad and Tobago's strategy suffered from the same level of vagueness.

The absence of any perceivable effort on the part of the other member states speaks to a level of malaise that is compounded by the failure of CARICOM to articulated or coordinate a regional effort.

CARICOM Cyber Security Initiatives after 2013

CARIMPACS was created to implement the CCSS within member states. However, the fragmented nature of the national efforts has only served to complicate the intended purpose of the Regional Intelligence Fusion Centre (RIFC) and the Joint Regional Communications Centre (JRCC) in coordinating the implementation of the CCSS.

⁶³ Global Forum on Cyber Expertise. "OAS Cyber Security Initiative," last accessed 25 March 2016. <http://www.thegfce.com/initiatives/cyber-security-initiative-in-oas-member-states>.

⁶⁴ Symantec Corporation, Latin American and Caribbean Cyber Security Trends, (Washington: OAS Press, 2014), p 7.

⁶⁵ Caribbean Community Secretariat, "Crime and Security Strategy" (Turkeyen: Guyana, 2013), 64 p.

⁶⁶ Ministry of Science, Technology, Energy and Mining. National Cyber Security Strategy. (Kingston: GoJ Printing Press, 2014), 39 p.

Under the auspices of the OAS CARICOM nation states have pursued cyber security initiatives. The problem with this approach is that the countries have not made much progress towards becoming proactive to date.⁶⁷ This failure has been primarily because the efforts by each member state have been duplicitous and inadequate. This can be seen in the efforts of countries like Trinidad and Tobago, Jamaica, Guyana and Barbados. Each is trying to do the same thing with the same pool of resources with varying degrees of achievement and success.⁶⁸

Proactive Security Proposal

This paper argues that a less duplicitous approach, coordinated by CARICOM, which taps the existing capacities and strengths within member states has a greater chance of achieving a more holistic cyber security stance. Hence there would be a more integrated security strategy.⁶⁹ This would allow for focused efforts from the RIFC in prevention and detection efforts and the JRCC in response and recovery.

Some of the key activities to be tackled in this effort include the creation of a Regional critical systems catalogue, implementing automated tools to build regional situational awareness across governments of IT systems and services, and addressing the jurisdictional, legal and policy changes necessary to enable the effective information sharing across states.

In avoiding gaps in the endstate across nations, the definition of Proactive Cyber Defence as offered by Bell Canada is suggested for adoption by CARICOM:

...acting in anticipation to oppose an attack against computers and networks. It represents the thermocline between purely offensive and defensive action; interdicting and

⁶⁷ Symantec Corporation, Latin American and Caribbean Cyber Security Trends, (Washington: OAS Press, 2014), 47.

⁶⁸ Ibid.

⁶⁹ Caribbean Community Secretariat, Strategic Plan for the Caribbean Community 2015 – 2019: Repositioning CARICOM (Turkeyen: Gyuana, 2014), 23.

disrupting an attack or a threat's preparation to attack, either pre-emptively or in self-defense.⁷⁰

The variable and changing boundaries between the three core activities of CNO could be representative of the thermocline. Additionally, it should be borne in mind that there are links and interdependencies among these activities. Thus the aim of Proactive Cyber Defence could be to give CARICOM a level of cooperative sophistication that will enable its organs to treat with potential issues before they can affect member states. It would require a clear governance framework, with jurisdictional support in each territory particularly where CND activities transition to CNE or CNA efforts.

Legal Ramifications

Any CNO implementation must take into account the existing bailiwick of the Laws of Armed Conflict (LOAC).⁷¹ This position is further strengthened by Mark Shulman when he advocates that since the ideas of military necessity, proportionality and discrimination apply to cyber-attacks, international courts should be allowed the flexibility of building a body of case law over time.⁷²

Article 51 of the UN Charter allows for self-defence:

Nothing in the present Charter shall impair the inherent right of collective and individual self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.⁷³

⁷⁰ Bell Canada. Security, Intelligence, Law Enforcement, Public Safety and National Defence Research: Bell Canada Security Story, no pagination.

⁷¹ Directorate of Law Training, ed., B-GG-005-027/AF-022, Collection of Documents on the Law of Armed Conflict (Ottawa: Dept. of National Defence, 2005).

⁷² Mark R. Shulman, "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1998-1999), 939.

⁷³ United Nations General Assembly, *Charter of the United Nations*. (New York: UN, 1948). Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51. Last accessed 18

It must be borne in mind that CARICOM is not a state. Hence much of what could be achieved would have to be at the invocation of the right to collective self-defence.

Responsibilities

The Caribbean Nations Security Conference (CANSEC)⁷⁴ already provides a platform for the security apparatuses of CARICOM to collaborate. However, the military and constabulary chiefs that attend the conference are not incorporated into any formal grouping. The role of this annual conference could however be expanded to include the operational level supervision of activities within the cyber environment as a “warfighting” domain. Thus the extant cyber operations capabilities existing in member states, with direct applicability to the creation of a CARICOM cybersecurity strategy, could be marshalled into a robust regional CNO capability.

The role of CARICOM is to regulate state on state interaction within the alliance. From a cyber standpoint the assistance of cyber service providers and even individuals is required to meet this challenge. This effort begins by having the necessary policies and capabilities in place across jurisdictions and requires focused planning and funding. Intergovernmental collaboration is required to address unresolved organizational, governance, technical, and jurisdictional issues. Individual Government Operations Centres (GOC)⁷⁵ currently attempt to integrate Cyber

March 2016. <http://www.un.org/aboutun/charter/chapter7.shtml>; “Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.”

⁷⁴ The Caribbean Nations Security Conference (CANSEC) is comprised of all Military chiefs from Caribbean countries as well as the United States Southern Command (US SOUTHCOM) and commissioners of police where the state has no standing military. Annually the position of chair rotates among represented countries with the exception of the United States Southern Command. Additionally, the fact that non CARICOM countries are represented would have to be taken into account in operationalising the membership for CARICOM issues.

⁷⁵ GOCs such as the Joint Information and Operations Centre in Jamaica exist in member states. They are largely the result of bilateral agreements between the member state and an external organisation or military. Last accessed 08

incident reports from each country but lacks the mechanisms to do little more than high-level reporting and limited information sharing. Each government is responsible for CND of its own networks, while some are mandated in specific areas, Cyber criminality for example is a constabulary responsibility. Militaries, in some countries, are the only state apparatus with both the mandate and an existing CNO capability to conduct all three functions CND, CNE and CNA.

CARICOM has touted the creation of a Cyber Security Strategy (CCySS)⁷⁶ and an associated Cyber Crime Centre (CCCC)⁷⁷ as the preferred model to support the Region's vision of being proactive rather than reactive; however, this initiative is still just a concept. While more work is being accomplished in the policy realm, with the assistance of the OAS, integration of existing CARICOM capability remains a challenge to be resolved. The integration of intelligence and CNE capabilities from multiple GOCs including the Jamaica, Trinidad and Tobago, Barbados, Guyana and other CARICOM institutions is vital to the ability to determine the intent and the source(s) of Cyber-attacks. CARIMPACS can play a significant role in leading and integrating the implementation of CARICOM Cyber initiatives through its ability to generate economies of scale in contracting, security posture and requirements, experience in IT Service Management (ITSM), access to international intelligence sources, ability to perform research in support of CNO, and its relationship with GOCs.

May 2016. <http://www.forces.gc.ca/en/news/article.page?doc=strengthening-the-core-of-the-jamaica-defence-force/ht17dcd>

⁷⁶ Caribbean Community Secretariat, *Strategic Plan for the Caribbean Community 2015 – 2019: Repositioning CARICOM* (Turkeyen: Gyuana, 2014), 23.

⁷⁷ Ibid.

CHAPTER IV – POTENTIAL CNO CONTRIBUTIONS TO MEET CCSS MISSIONS

For the first time, the role of Cyber is articulated in a CARICOM paper and demands new levels of performance for the region to be responsive to a wide range of potentially simultaneous core missions.⁷⁸ Despite the looming challenges with equipment, personnel training and staffing requirements several initiatives have sought to redress the shortages of trained personnel. That being said, the CARICOM Strategic Plan's tasks place additional demands upon the existing structures and resources which will definitely need to be augmented.⁷⁹ The extent of the personnel gap remains a question to be answered, but the CARICOM's CNO force generation requirements would have to be increased to facilitate the proposed CCySS, particularly with the increased focus on regional issues that require more collaboration and integration among sovereign states. This may involve posting individuals to other countries in a liaison capacity. However, the increased maintenance costs of such postings make them unattractive to member states.⁸⁰

⁷⁸ CARICOM Secretariat. CARICOM. "Strategic Plan for the Caribbean Community 2015 – 2019: Repositioning CARICOM" (Turkeyen, Gyuana), July 2014, 23.

⁷⁹ According to Brigadier Rocky Meade, Deputy Chief of Defence Staff, Jamaica Defence Force, Organisations such as CARIMPACS, RIFC and JRCC as well as the other 25 institutions of CARICOM suffer significant sustainment challenges. This stems primarily from member states failure to fulfill obligations for resourcing as agreed at inception.

⁸⁰ Ibid.

CHAPTER V – A SEMANTIC STATE FRAMEWORK

Principals

The European Union (EU) Collaborative Middleware for Monitoring Financial Critical Infrastructure (CoMiFin)⁸¹ is considered as the service model for the proposal of a Semantic State for collaborative CNO within CARICOM. There are three basic components used in the Semantic Room (SR) Abstraction in order to facilitate the processing and sharing of information with participating institutions in a specific room being referred to as members of that SR. The intent of the proposed framework is to expand this conceptual SR to represent a Semantic State (SS). The main components here would be CARICOM and its organs, member states and international partners.

Abstraction

This paper proposes that, CARICOM as a coordinating umbrella, represents the SS. Thus the abstraction would be centered on the following elements:⁸²

The contract. This would be the regulating criteria that determines ambit of the data/information processing and sharing services provided within the SS. Also captured would be the prevention, detection, response and recovery guidelines and the confidentiality, integrity and availability (CIA) requirements of the SS. The contract would also, of necessity, contain the hardware and software requirements for admittance into membership of the SS;

⁸¹ Roberto Baldoni and Gregory Chockler. Collaborative Financial Infrastructure Protection. (Springer, 2012).

⁸² Ibid.

The objective. The SS would require strategic objective(s) to be articulated. One such could be a CARICOM Strategy for cyber security. Additionally, lines of operation could be established in support of the objective(s).

The deployments. The SS would be associated with different technologies, thereby allowing for multiple and varied SS deployments. This abstraction of the SS is intended to make it flexible enough to have an adaptive logical and functional implementation. Of particular importance would be the processing and sharing approaches to system implementation. Chief among these would be the centralized approach where central points like the RIFC or the JRCC could be resourced and used as a hub,⁸³ a decentralized approach where the processing load and sharing responsibility are evenly distributed among members of the SS (for example, a DHT-based scenario), or a hierarchical approach where different members have different processing and sharing responsibilities and some level of pre-processing takes place. The pre-processed information is then

passed to other members for additional processing.

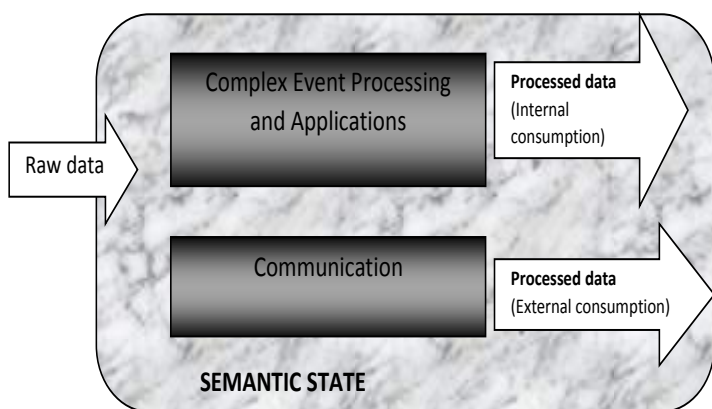


Fig. 1. The Semantic State Abstraction

⁸³ Roberto Baldoni and Gregory Chockler. Collaborative Financial Infrastructure Protection. Springer, 2012.

As shown in this fig. 1, the SS abstraction supports the deployment of two components termed Complex Event Processing and Applications, and Communication⁸⁴ which can vary from deployment to deployment depending on the software technologies employed to implement the deployment's processing and sharing logic, and a set of management components, that together form the overarching framework in Figure 1 and that are exploited for SS management purposes (e.g., management of the membership, monitoring of the SS operations). SS members can inject raw data into the SS. Raw data may include real-time data, inputs from human beings, stored data (e.g., historical data), queries, and other types of dynamic and/or static content that are processed in order to produce complex processed data. Raw data are properly managed in order to satisfy privacy requirements that can be prescribed by the SS contract and that are crucial in order to effectively enable a collaborative environment among different, and potentially competitive, financial institutions.

Processed data can be used for internal consumption within the SS: in this case, derived events, models, profiles, blacklists, alerts and query results can be fed back into the SS so that the members can take advantage of the intelligence provided by the processing (Figure 1). SS members can, for instance, use these data to properly instruct their local security protection mechanisms in order to trigger informed and timely reactions independently of the SS management. In addition, a (possibly post-processed) subset of data can be offered for external consumption. SSs in fact can be willing to make available for external use their produced processed data. In this case, in addition to the SS members, there can exist clients of the SS that cannot contribute raw data directly to the SS but can simply consume the SS processed data for

⁸⁴ Roberto Baldoni and Gregory Chockler. Collaborative Financial Infrastructure Protection. (Springer, 2012).

external consumption (Figure 1). SS members have full access to both the raw data members agreed to contribute to by contract, and the data being processed and thus output by the SS. Data processing and results dissemination are carried out by SS members based on obligations and restricts specified in the above mentioned contract.

Semantic State Governance Layer

The proposed governance structure for the CARICOM SS would seek to leverage the existing hierarchies within CARICOM and implement structure to improve robustness where there are gaps. The CARICOM Heads of Government (HoG) through the Secretariat would have overall control of the CNO capabilities within SS. Thus it would have executive responsibility at the strategic/political level. The decisions regarding the operationalization of the deployments would be responsibility of the CANSEC leadership. It would be charged with making recommendations regarding CND, CNE or CNA actions to the CARICOM HoG. Additionally, it would have implementation at the operational level. GOCs would have tactical level implementation authority.

An instance of possible application is detailed in the attached appendix.

CHAPTER VI – CONCLUSION

This paper argues that CARICOM must deliver the Cyber Operations capabilities required to support the CCSS strategy in the Cyber environment. It described the Cyber environment in a Caribbean context and Cyber Operations capabilities were shown to be essential in determining the adversarial intent and the identity of Cyber attackers. The lead tactical implementer to address specific Cyber threats would depend on the intent and the identity of the perpetrators due to the implications regarding information gathering and sharing imposed by the various jurisdictions. Because of the complex interconnectivity between the security and defence mandates and apparatuses, a solution to the integration challenges in dealing with Cyber-attacks is needed. There is no CNO capability that is currently a clear leader in all Cyber functions though the OAS is assisting with the task of developing the cyber initiatives in individual member states. The Cyber governance and doctrinal issues in CARICOM are finally receiving the much needed attention, as the constabularies, militaries and government senior leadership have an increased awareness of the Cyber threats. The proposed semantic framework recommends that the responsibility for Cyber Operations be distributed and tiered with GOCs having tactical responsibility given their track record and immediate availability to respond. Key to quickly harnessing the available Cyber resources efficiently is the need to build upon the existing niche specialization in specific countries and the sharing of existing capacity. GOCs would therefore be able to concentrate on their prime mission, which is to deal with defending states from network attacks, as outlined in the existing CCSS and the proposed CCySS.

Militaries and constabularies role in the Cyber environment against their core missions assigned in CCSS must also be assessed in a quantitative manner to identify the resources

required within to operationalize CARICOM and national funding within the respective budget cycles. The member states have limited time and qualified personnel to provide an assessment of the capability gap to insert true CNE and CNA capabilities within the GOCs to complement the existing CND capability. The assessment will need to identify the required increase in resource levels for GOCs to operate the full complement of CNO capabilities (CND, CNE and CNA) on a 365/24/7 basis. In the meantime, the Cyber training and education plans touted by CARICOM and the OAS should be implemented immediately to improve the force generation capacity within the regional security apparatuses and eventually aim to also extend it to GOCs, OGDs and vetted corporate entities to address their CND capability gap.

The research supporting this paper was based on the limited unclassified data available regarding the Cyber threats and vulnerabilities, CARICOM may find value in conducting a separate analysis at the classified level to gain a full appreciation of the Cyber environment and its implications beyond those affecting the member states' ability to answer the requirements of CCSS.

In summary, CARICOM's Cyber semantic gap can best be described as lessening. This is due in part to a growing momentum of policy development, financial support, intellectual and legal debate, intergovernmental cooperation and general awareness about Cyber issues. It is however currently not as prepared as it should be to address the existing and growing Cyber threats and should be more proactive, lest the region suffers a devastating Cyber-attack while it is still determining available capacity. CARICOM has never had to deal with the hard lessons that states like Estonia learned, if it acts expeditiously it can reduce its Cyber semantic gap.

Bibliography

- Adee, Sally “The Hunt For The Kill Switch”, Spectrum IEEE, Vol. 45, Issue 5, (May 2008).
Last accessed 8 April 2016.
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4505310;
- Baldoni, Roberto and Chockler, Gregory. Collaborative Financial Infrastructure Protection. (Springer, 2012).
- Burnet, Peter “The Vital Role of Critical Information Infrastructure Protection (CIIP) in Cybersecurity”, Report on Cybersecurity and Critical Infrastructure in the Americas, (Trend Microsystems and OAS), 2015. p 13.
- Bell Canada. “Carrier Grade Threat and Vulnerability Intelligence”, December 2008, 1.
- Bell Canada. Security, Intelligence, Law Enforcement, Public Safety and National Defence Research: Bell Canada Security Story, no pagination.
- Caribbean Community Secretariat, “Crime and Security Strategy” (Turkeyen: Guyana, 2013), 64 p.
- Caribbean Community Secretariat, Strategic Plan for the Caribbean Community 2015 – 2019: Repositioning CARICOM (Turkeyen: Guyana, 2014), 23.
- Caribbean Community Secretariat, “Revised Treaty of Chaguaramas Establishing The Caribbean Community including the CARICOM Single Market and Economy”, Last accessed 5 May 2016. https://issuu.com/caricomorg/docs/revised_treaty_text.
- Cavelty, Myriam Dunn Cyber-Security and Threat Politics : US Efforts to Secure the Information Age (Milton Park, Abingdon, Oxon ; New York: Routledge, 2008), 18.
- Chuka, Neil “Confusion and Disagreement: The Information Operations Doctrine of the US, the US, AUS, CA and NATO”, (Master’s Thesis, Royal Military College of Canada, 2007), 8.
- Concise Oxford Dictionary Online. Last accessed 30 March 2016
http://www.askoxford.com/concise_oed/environment?view=uk
- Department of Defence Instruction 8100.3, Department of Defense Voice Networks. Last accessed 16 April 2016, <http://www.dtic.mil/whs/directives/corres/pdf/810003p.pdf>.
- Department of National Defence. B-GG-005-004/AF-010, CF Information Operations, (Ottawa: DND Canada, 1998-04-15), 1-2.
- Department of State. “Caribbean Basin Security Initiative,” last accessed 5 May 2016, <http://www.state.gov/p/wha/rt/cbsi/>

Directorate of Law Training, ed., B-GG-005-027/AF-022, Collection of Documents on the Law of Armed Conflict (Ottawa: Dept. of National Defence, 2005).

Gallagher, Sean “The Right Stuff for Cyber Warfare”, Defense Systems, (20 October 2008). Last accessed 16 February 2016. <http://defensesystems.com/Articles/2008/10/The-right-stuff-for-cyber-warfare.aspx>;

Global Forum on Cyber Expertise. “OAS Cyber Security Initiative,” last accessed 25 March 2016. <http://www.thegfce.com/initiatives/cyber-security-initiative-in-oas-member-states>.

Jamaica Defence Force, Jamaica Defence Force Tasks. Last Accessed 23 March 2016, <http://www.jdfmil.org/jdfTask/tasks.php>

Jessop, David “New Threats to Caribbean Cyber Security”, *View From Europe*, (August 2015): https://www.google.ca/search?q=david+jessop+new+threats+to+caribbean+cyber+security&ie=utf-8&oe=utf-8&gws_rd=cr&ei=wb8xV4b5IaSCjwTrr7ngCg#q=david+jessop+new+threats+to+caribbean+cyber+security+view+from+europe

Keith Stewart. DRDC Toronto. “Influence Operations: Historical and Contemporary Dimensions”, DRDC Toronto CR-2007-126, 31 July 2007. Last accessed 15 April 2016. <http://cradpdf.drdc.gc.ca/PDFS/unc69/p528894.pdf>

Leblanc, Sylvain and Knight, Scott. “Engaging the Adversary as a Viable Response to Network Intrusion”, Workshop on Cyber Infrastructure Emergency Preparedness Aspects, Ottawa, 21-22 April 2005; last accessed 20 February 2016 <http://tarpit.rmc.ca/knight/papers/IO%20Counter-measures.doc>.

Libicki, Martin C. and Rand Corporation, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge: Cambridge University Press, 2007), 8.

Ministry of Science, Technology, Energy and Mining. *National Cyber Security Strategy*. (Kingston: GoJ Printing Press, 2014), 39 p.

Natasha Solce, “The Battlefield of Cyberspace: The Inevitable New Military Branch – The Cyber Force”. *Albany Law Journal of Science and Technology*. #18 (2008), 305.

Richards, Jason “Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security”, *International Affairs Review*; last accessed 25 March 2016. <http://www.iar-gwu.org/node/65.html>.

Shulman, Mark R. "Discrimination in the Laws of Information Warfare," *Columbia Journal of Transnational Law* 37 (1998-1999), 939.

Symantec Corporation, *Latin American and Caribbean Cyber Security Trends*, (Washington: OAS Press, 2014), 91 p.

Symantec Corporation, Internet Security Threat Report Trends for July–December 07, Volume XIII, Published April 2008, 30.

United Nations General Assembly, *Charter of the United Nations*. (New York: UN, 1948).

Appendix 1

Figure 1 illustrates what could be a specific instance of a CARICOM SS which is capable of preserving the privacy of sensitive data during collaborative events processing. The architecture consists of two main components: a so-called Edge Gateway, and a Collaborative Processing System (CPS). The edge gateway transforms raw data into events, here as CPS detects anomalous behaviors. These components are used in three different phases of the data processing. The phases work as in a pipeline and are described next.

Pre-processing phase

The Edge Gateway could be located at the service provider site or the GOC. It is responsible for (i) protecting sensitive data items, as prescribed by contracts service providers established with the contracting entity (see Figure 1), and (ii) injecting anonymized data to the Collaborative Processing System. The Edge Gateway component would be designed so as to embody two principal modules; namely, the privacy-enabled pre-processing and data dissemination modules.

Privacy-enabled pre-processing module.

In the privacy-enabled pre-processing module, raw data of service providers are pre-processed by filtering unnecessary data and/or aggregating data according to specific formats necessary for the successive private event processing phase (see Reconstruction Unit for details). In addition, aggregated data are given to a privacy preserving algorithm which anonymizes sensible data according to specific contractual clauses.

The algorithm is based on the Shamir's (k, n) secret sharing scheme⁸⁵, which permits parties to share a secret 's' among 'n' entities in a way that the secret can be easily reconstructed if and only if any 'k' out of the 'n' participants make their shares available, where $k \leq n$ provides the strength of the scheme. This is achieved by generating a random polynomial 'f' of degree $k - 1$ defined over a prime field Z_p , with $p > s$ and such that $f(0) = s$. The polynomial is used to generate n different shares, $s_1; s_2, \dots, s_n$, where $s_i = f(i)$. The vector of shares is denoted by $[s]$. The secret can be reconstructed exploiting the Lagrange interpolation technique. The architecture assumes that a certain number $w < n$ of participants are semi-honest (Businesses and individuals in the extranet); that is, they do follow the collaborative processing protocol, but they are "curious" and attempt to infer as much information as possible from the computation itself. In principle, semi-honest participants can even coordinate themselves in order to increase the chances of getting private data. In order to neutralize the semi-honest activities the scheme sets $k = w + 1$. The privacy preserving scheme embodied in the Edge Gateway first divides the aggregated data into two parts, a sensitive data part s and a non-sensitive part u . Shamir's scheme is then applied to s and the produced list of shares $[s]$ is sent to the data dissemination module together with the u part.

⁸⁵ A. Shamir. How to share a secret. *Communications of the ACM*, 22:612-613, 1979.

Data Dissemination module.

This module is in charge of disseminating private data to all the entities in the form of events. The dissemination occurs periodically, i.e., every fix time window. The beginning and end of each period is demarcated through special signaling messages. The module sends elementary information in the form of a triple $(\text{hash}([s]); s_0; u)$, where $\text{hash}()$ is a perfect hash function, i.e., a function with no collisions. It is worth noting that the hash function takes all the shares as its argument: for any two secrets s, t , $\text{hash}([s]) = \text{hash}([t])$ iff $s = t$. For the purpose of data ordering, the data dissemination module of service provider i manages a vector seq_{ij} of sequence numbers associated with the participant j , which is reset at the beginning of a new dissemination phase. The entry seq_{ij} represents the sequence number of the last pair sent by i to j and it is increased by one unit before each transmission. Each triple $(\text{hash}[s], s_j, u)$ sent by the data dissemination module of service provider i to Participant j is tagged with the pair (i, seq_{ij}) . It is assumed that all the communication channels are secure, FIFO and reliable. The tuple $(i, \text{seq}_{ij}, \text{hash}[s], s_j, u)$ defines an event.

Private processing phase

The Collaborative Processing System (CPS) is responsible for (i) collecting private data sent by Edge Gateways of service providers, (ii) properly aggregating and processing the private data and (iii) sending back a result of the computation in an unanonymized form to service providers. The CPS can be thought of as a federation of private clouds. Each private cloud is essentially a deployment by a service provider and deployed for the sake of collaborative complex data processing. A private cloud consists of the set of hardware and software resources made available by the provider. It communicates with other private clouds in the federation only during the reconstruction phase (see below) using secure channels. Within a private cloud two processing units can be identified, as shown in Figure 1: a private processing unit and a reconstruction unit.

Private processing unit.

The goal of this unit is to aggregate and correlate private large datasets coming from the Edge Gateways and to notify anomalies to all the participants. In this design, the j^{th} private processing unit receives events $(i, \text{seq}_{ij}, \text{hash}[s], s_j, u)$ from Edge Gateway i , $i = 1, \dots, n$. The private processing unit is constructed out of a distributed network of processing and storage elements hosted in the private cloud. As a share acts as a shadow of the original secret, any participant has all the necessary data to make correlations. The processing elements manipulate and aggregate those data as follows. The processing elements are components of the MapReduce framework⁸⁶: a centralized Job Tracker coordinates the execution of mappers and reducers on each resource of the private cloud through a collection of Task Trackers deployed on those resources. Mappers and Reducers process the data according to a specific processing logic. A high level query language is used in order to define the processing logic. The language compiles into a series of MapReduce jobs. Specifically, the language supports SQL-like query constructs that can be combined into flow and specify the data patterns to be discovered on the set of input data. A

⁸⁶D. Je_rey and S. Ghemawat. MapReduce: simplified data processing on large clusters. *Communication of the ACM*, 51(1):107-113, 2008.

query engine is in execution inside each private processing unit: the engine retrieves the data in the storage elements and aggregates them according to one or more SQL-like queries.

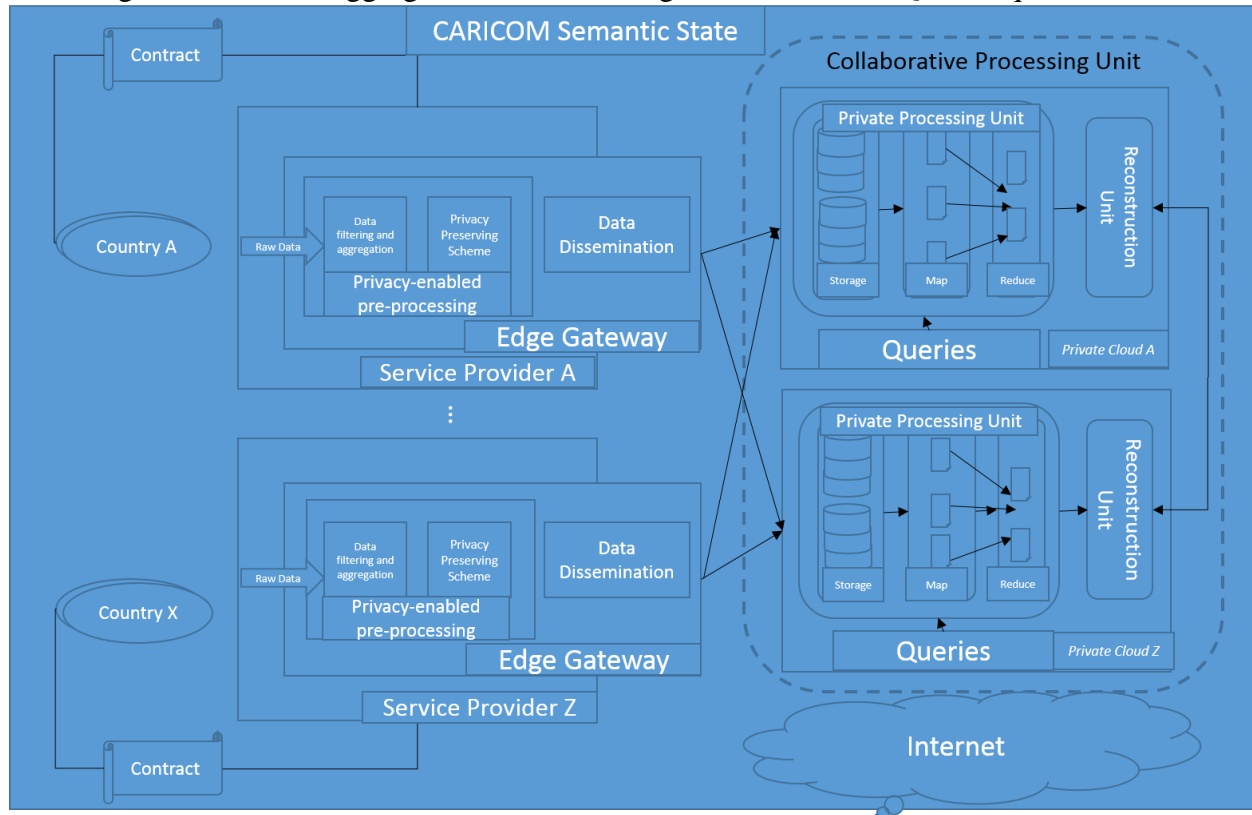


Fig. 1. Contract-based secure processing architecture

The final result from reducers is an ordered sequence of shares. The ordering is carried out by exploiting the “order by” constructs made available by the majority of SQL-like languages for data processing (e.g., HIVE⁸⁷, DMX⁸⁸). An external protocol could be also used as an alternative; it first orders the shares in groups, according to the lowest id of the entity from which the shares were sent, and then inside a group it orders them according to the sequence number of the shares.

Reconstruction unit.

The reconstruction unit is responsible for communicating with the other reconstruction units of the private clouds of the federation in order to rebuild the secret. Each reconstruction unit sends the output of the query, i.e., an ordered list of shares, and waits for receiving a similar list from all the other participants. Each unit then applies the Lagrange interpolation algorithm to reconstruct the original secret. The reconstruction algorithm is organized as sequence of

⁸⁷ Apache Hive. Last accessed 10 May 2016

<https://cwiki.apache.org/confluence/display/Hive/Home;jsessionid=3C9869B95786EDE504F7D1B43D1EA895#Home-ApacheHive>.

⁸⁸ Microsoft Corporation. Data Mining Extensions (DMX) Reference. Last accessed 10 May 2016.

<https://msdn.microsoft.com/en-us/library/ms132058.aspx>.

reconstructions. The first interpolation is applied using the first share in the lists received from the participants, the second interpolation is applied using the shares in the second position, etc.