Mohammed, Melanie

From: Policy Connection / Connections politiques

Sent: March 28, 2011 11:02 AM

To: Flack, Graham

Cc: Kubicek, Brett; Wadasinghe, Cheryl; Lee, Jennifer; Dakka, Iyad; Mohammed, Melanie; Charlton, Maxwell

Subject: FW: Policy Connection Cyber Series: Modern Warspace

Attachments: PS-SP-#364952-v1-Memo_to_the_AsDM_re__Policy_Connection_Cyber_Series__Modern_Warspace.DOC; 2011-03-02_DND_Modern_Warspace.ppt

UNCLASSIFIED

MEMORANDUM TO THE ASSOCIATE DEPUTY MINISTER

POLICY CONNECTION CYBER SERIES: MODERN WARSPACE

ISSUE

The purpose of this note is to provide a summary of the March 2, 2011 cyber seminar regarding Modern Warspace, which was jointly hosted by Policy Connection and Public Safety Canada's Policy and Issues Management Division, and presented by the Department of National Defence (DND).

A previous memorandum providing further context regarding the seminar is attached. A copy of the presentation given by DND is also attached for your information.

SUMMARY

The cyber environment, as defined by DND/Canadian Forces, consists of the interdependent network of information technology structures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers – as well as the software and information stored within.

From a national security perspective, there is a wide range of activities that occur in the cyber environment, ranging from defensive to offensive. Defensive cyber operations are typically said to include actions taken in cyberspace to protect one's own computers and networks from intrusion. Offensive cyber operations could include actions taken to deny an adversary's use of information stored on the target nation's computers and networks, or actions to disrupt communications or other systems (e.g., critical infrastructure). Cyber operations are also frequently used for intelligence collection purposes.

The most sophisticated cyber threats come from the intelligence and military services of foreign states. These attackers are well resourced, patient and frequently sophisticated. Their purpose is to gain political, economic, commercial or military advantage, and they typically target governments and private businesses. Reports from Canada and across the world confirm that these attacks have succeeded in stealing industrial and state secrets, private data and other strategically valuable information. Some foreign states have declared publicly that cyber attacks are a central element of their military strategy, and have been accused of using cyber attacks to support military operations. The evolution of cyber attack tools and techniques has accelerated dangerously in the recent past.

DISCUSSION

During the discussion period, questions were raised regarding the recent reports of cyber incursions on Government systems, namely at the Treasury Board Secretariat, Finance Canada and Defence Research and Development Canada. Some felt that the incident was a cyber attack, while other felt that it fell within the more tactical concept of cyber espionage. Given that the exploitations were disruptive and that information was stolen from the compromised systems, some felt that it constituted a deliberate attack on Government networks. Others felt that the Government overreacted by shutting off the Internet at the affected departments, and that by not taking any offensive measures, the Government is essentially inviting further cyber espionage. There was a common sense of frustration in the room that the Government has not been more open and transparent regarding the attacks, nor regarding response and

recovery measures.

The discussion then transitioned to the need for the Government to declassify its intelligence in the context of cyber security. As is the case with many Government departments, DND guards intelligence regarding cyber attacks and response mechanisms in the military realm out of fear that such information could provide adversaries, or even curious citizens, with the tools to launch attacks against Government, or even civilian, systems. DND spoke positively about the need to declassify their intelligence and share it more broadly across Government and with industry. Doing so could significantly help in protecting the vital assets of private and critical infrastructure sectors.

CONCLUSION

The seminar was well-received among participants, who were encouraged to participate in the April 2011 seminar on "Ethical Hacking and Cyber Espionage." Further information regarding that seminar will follow under separate cover.

Prepared by: Melanie Mohammed, 613-991-2700

Attachments: (2)

c.c.: Lynda Clairmont, Assistant Deputy Minister, EMNS

UNCLASSIFIED

Date: January 31, 2011

RDIMS No.: 364952

MEMORANDUM FOR THE ASSOCIATE DEPUTY MINISTER

POLICY CONNECTION CYBER SERIES: MODERN WARSPACE

(Information only)

ISSUE

Policy Connection and Public Safety Canada's Cyber Policy Division are jointly organizing a series of cyber security-related seminars, which will take place during the first quarter of 2011. The seminars will provide a forum for capacity building and broad policy discussions regarding cyber security. Policy Connection and the Cyber Policy Division share a common interest in engagement and policy development, and are therefore of the view that the joint seminars demonstrate a meaningful way to achieve shared goals.

The first seminar, which will take place from 12:30 to 14:30 on February 23, 2011, will be regarding Modern Warspace, and will be presented by the Department of National Defence (DND).

BACKGROUND

In December 2010, given the October 3, 2010 launch of *Canada's Cyber Security Strategy*, the Cyber Policy Division made an informal proposal to Policy Connection to jointly host a series of cyber security-related seminars in early 2011. The proposed topics of discussion included Modern Warspace, cyber espionage, ethical hacking and information sharing.

Over the course of the month, Policy Connection and the Cyber Policy Division collaborated to engage DND and the Department of Justice as lead presenters for the seminars.

CURRENT STATUS

DND has agreed to make a presentation regarding Modern Warspace on February 23, 2011. Using a five-layer model to describe the virtual and physical realms of warfare, DND will explore the necessity of a whole-of-Government

.../2

approach in the global commons of space and cyber; the required thinking regarding the notion of deterrence in the cyber environment; and the importance of public-private, interagency, and coalition partnerships.

Invitations to the seminar will be sent to Public Safety Canada officials and members of the Directors General Interdepartmental Committee on Cyber Security (DG Cyber), which is chaired by the Director General, National Cyber Security Directorate, during the week of January 31, 2011. To ensure insightful and thought-provoking discussions, EX-01 and EX minus 1 policy makers from Public Safety Canada will be identified by Directors General within the Department. The members – or their EX-01 and EX minus 1 delegates – of DG Cyber, will be also be invited to participate.

CONSIDERATIONS

Public Safety Canada is the lead department for *Canada's Cyber Security Strategy*. The Department is responsible for engaging federal partner departments and agencies under the Strategy to develop policies to support cyber security, and for promoting awareness to achieve a culture of cyber security consciousness among Canadians. Public Safety Canada also coordinates the implementation of the Strategy across the Government of Canada.

In hosting these seminars jointly with Policy Connection, the Cyber Policy Division is demonstrating strong Public Safety Canada leadership among its partners in the context of implementation of *Canada's Cyber Security Strategy*.

CONCLUSION

Following the February 23, 2011 seminar regarding Modern Warspace, Policy Connection will provide you with a summary of the discussion.

Should you require additional information, please do not hesitate to contact Jean-Thomas Nicole of Policy Connection at 613-990-3239, or Melanie Mohammed, Policy Analyst, Cyber Policy Division, at 613-991-2700.

Policy Connection/mm

National Defence
Défense nationale

DND: Modern Warspace

LCol Francis Castonguay
CF Cyber Task Force

2 March 2011

The Cyber environment is....

"The interdependent network of information technology structures, including the Internet, telecommunications networks, computer systems and embedded processors and controllers (including the software and information that reside within them)."

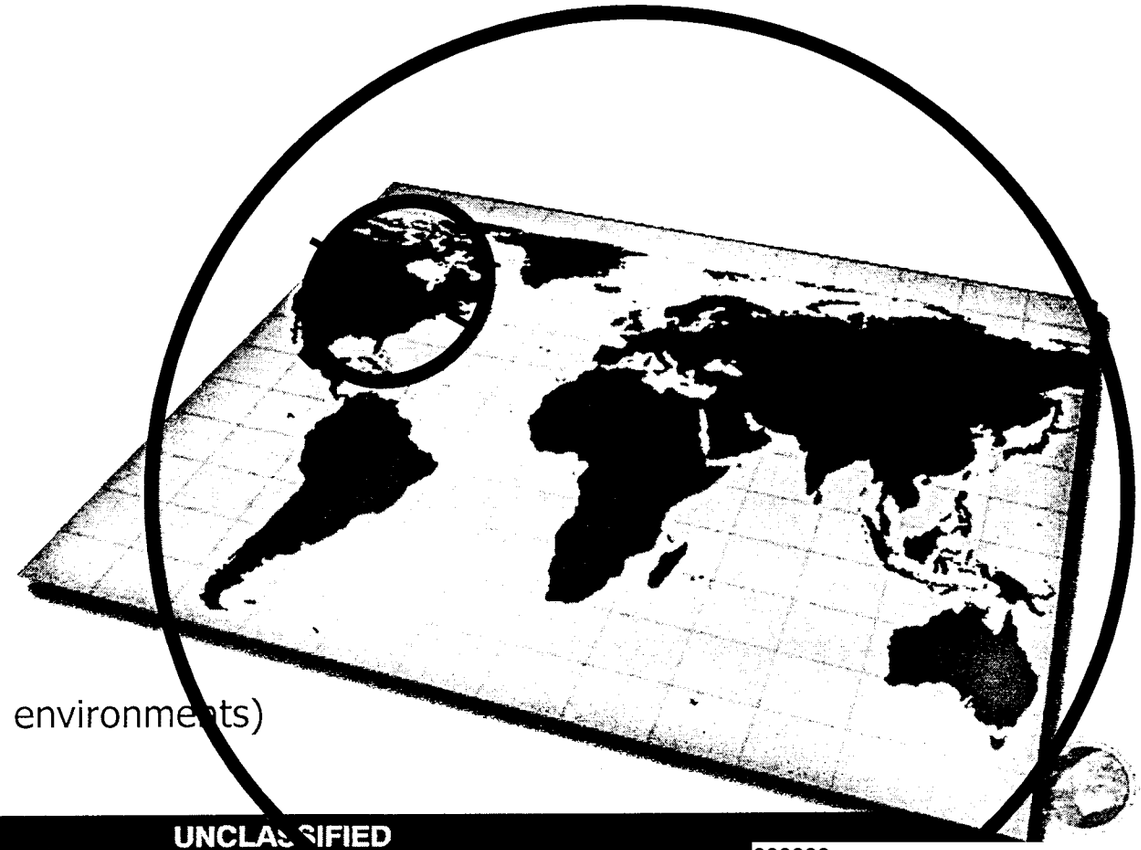
The Cyber environment is....

Cyber as a prefix is not useful to bring clarity. Activities such as Sabotage, Terrorism, Warfare take place in all environments, including the Cyber environment.

There is no normative code regarding whether the use of a multitude of (malicious) network activities represent a Use of Force, equivalent to an Armed Attack.

There is no clear/common understanding of the military role in the cyber environment across the spectrum of traditional military operations.

Understanding the Cyber Environment



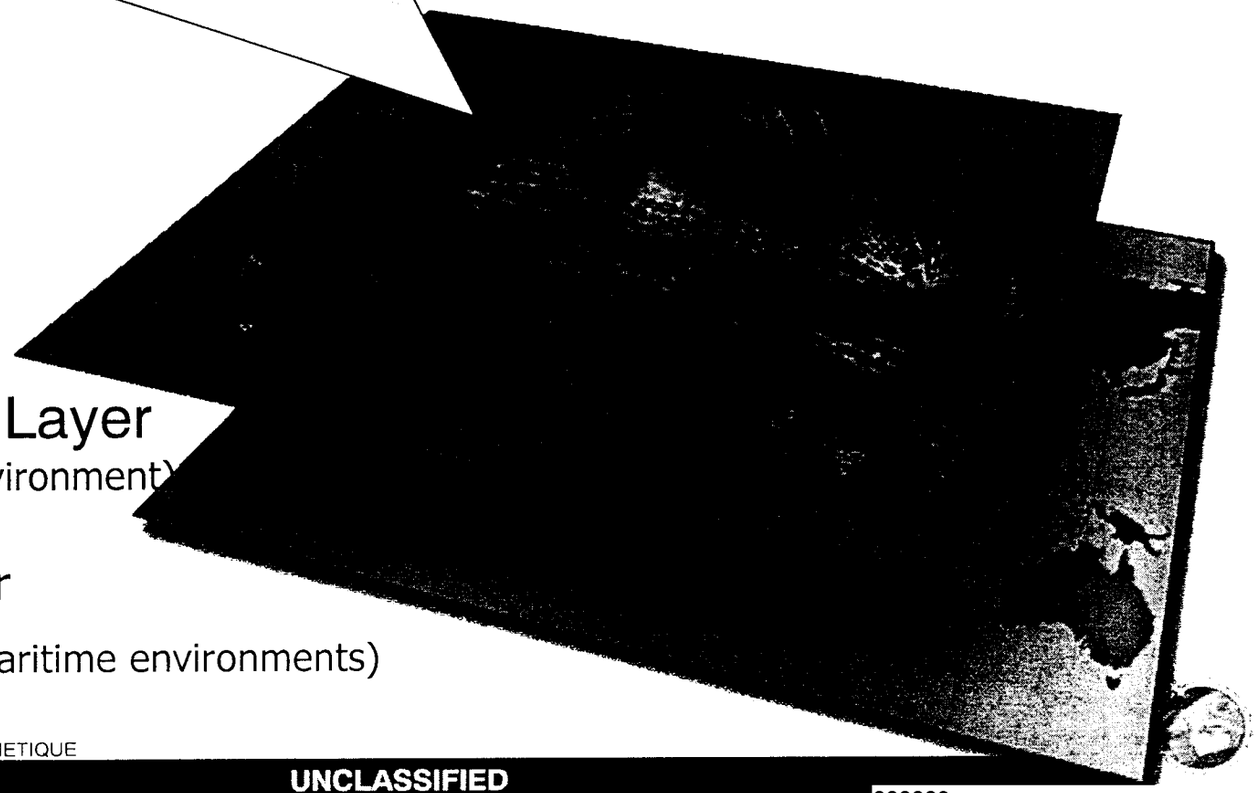
Geographic Layer

(Space, Air , Land, Maritime environments)

CYBER TASK FORCE
FORCE OPERATIONNELLE CYBERNETIQUE

Understanding the Cyber Environment

- A man-made physical operating environment (the key terrain)
- Constantly changing, resilient and transnational
- Is not virtual or a cloud – Cyber exists in physical devices



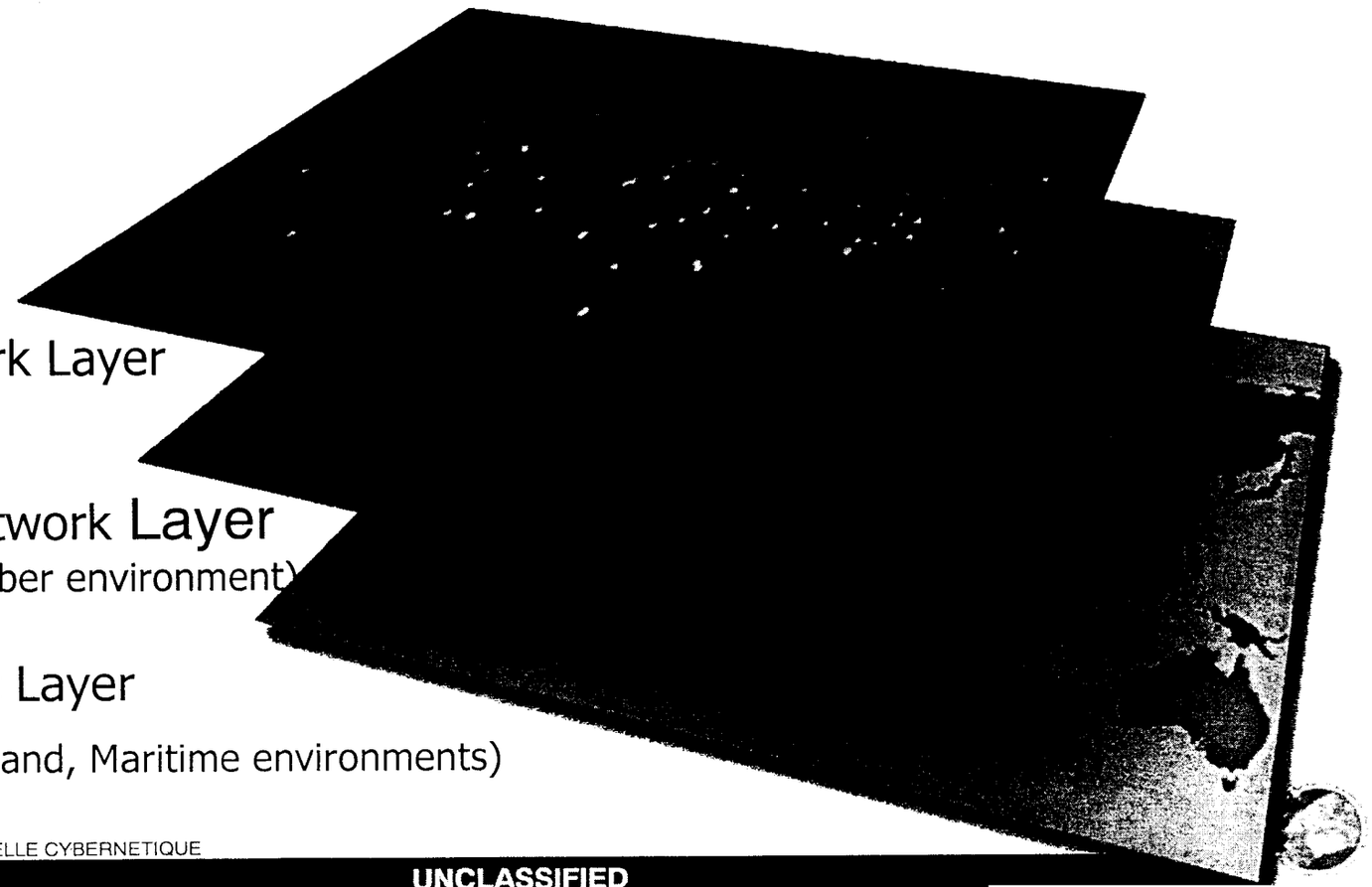
Physical Network Layer
(Man-made Cyber environment)

Geographic Layer

(Space, Air , Land, Maritime environments)

CYBER TASK FORCE
FORCE OPERATIONNELLE CYBERNETIQUE

Understanding the Cyber Environment



Logical Network Layer

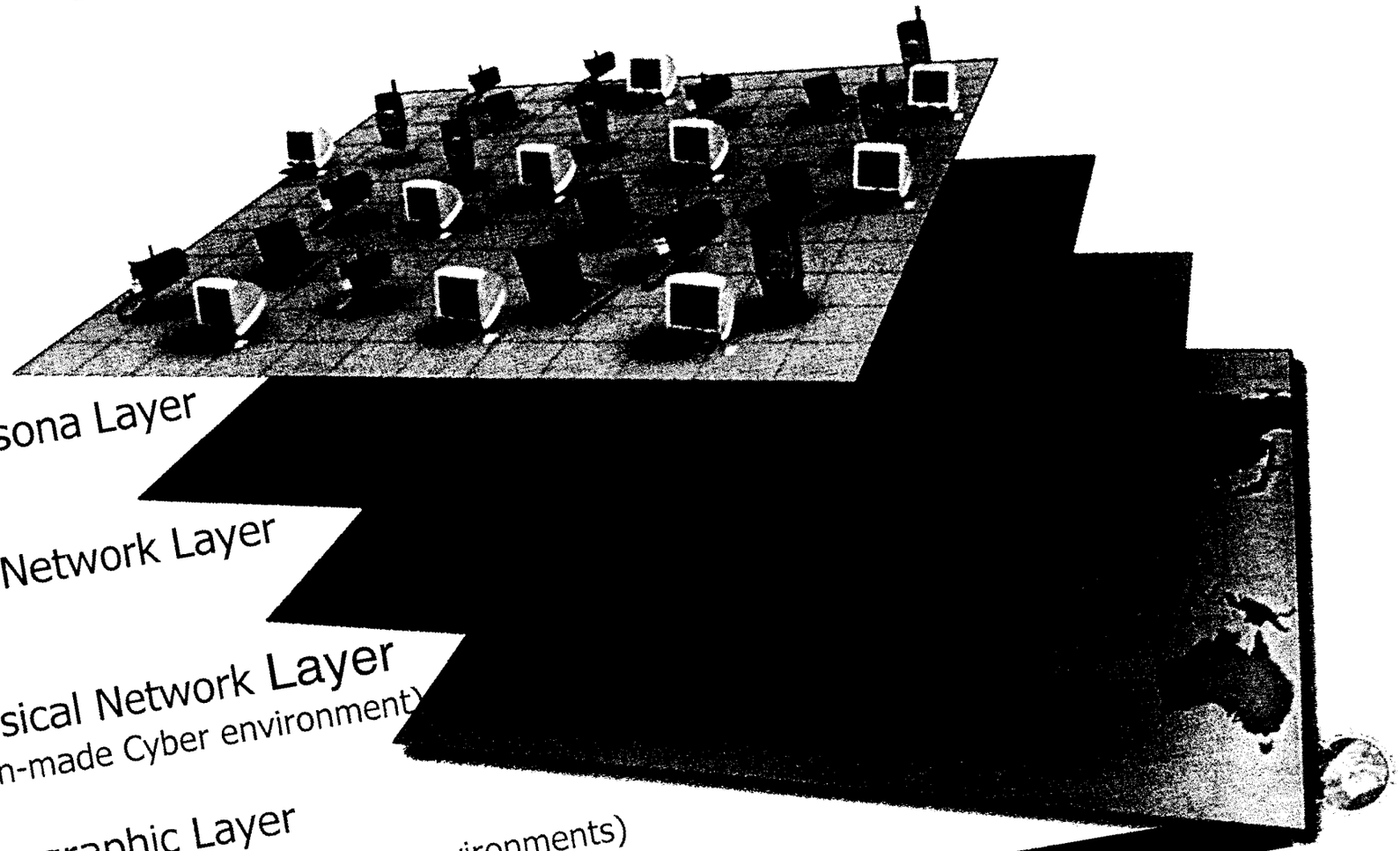
Physical Network Layer
(Man-made Cyber environment)

Geographic Layer

(Space, Air , Land, Maritime environments)

CYBER TASK FORCE
FORCE OPERATIONNELLE CYBERNETIQUE

Understanding the Cyber Environment



Cyber Persona Layer

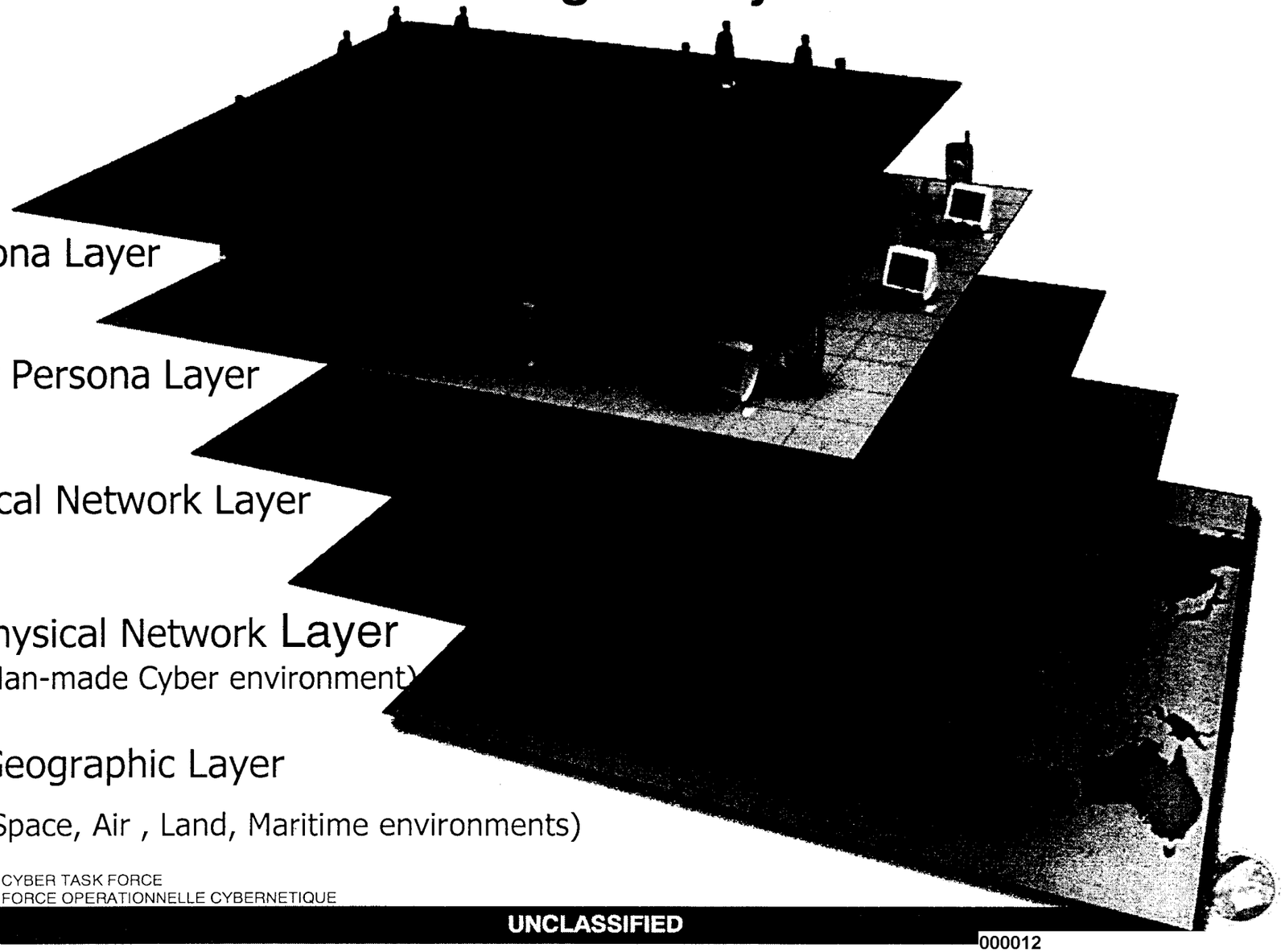
Logical Network Layer

Physical Network Layer
(Man-made Cyber environment)

Geographic Layer
(Space, Air , Land, Maritime environments)

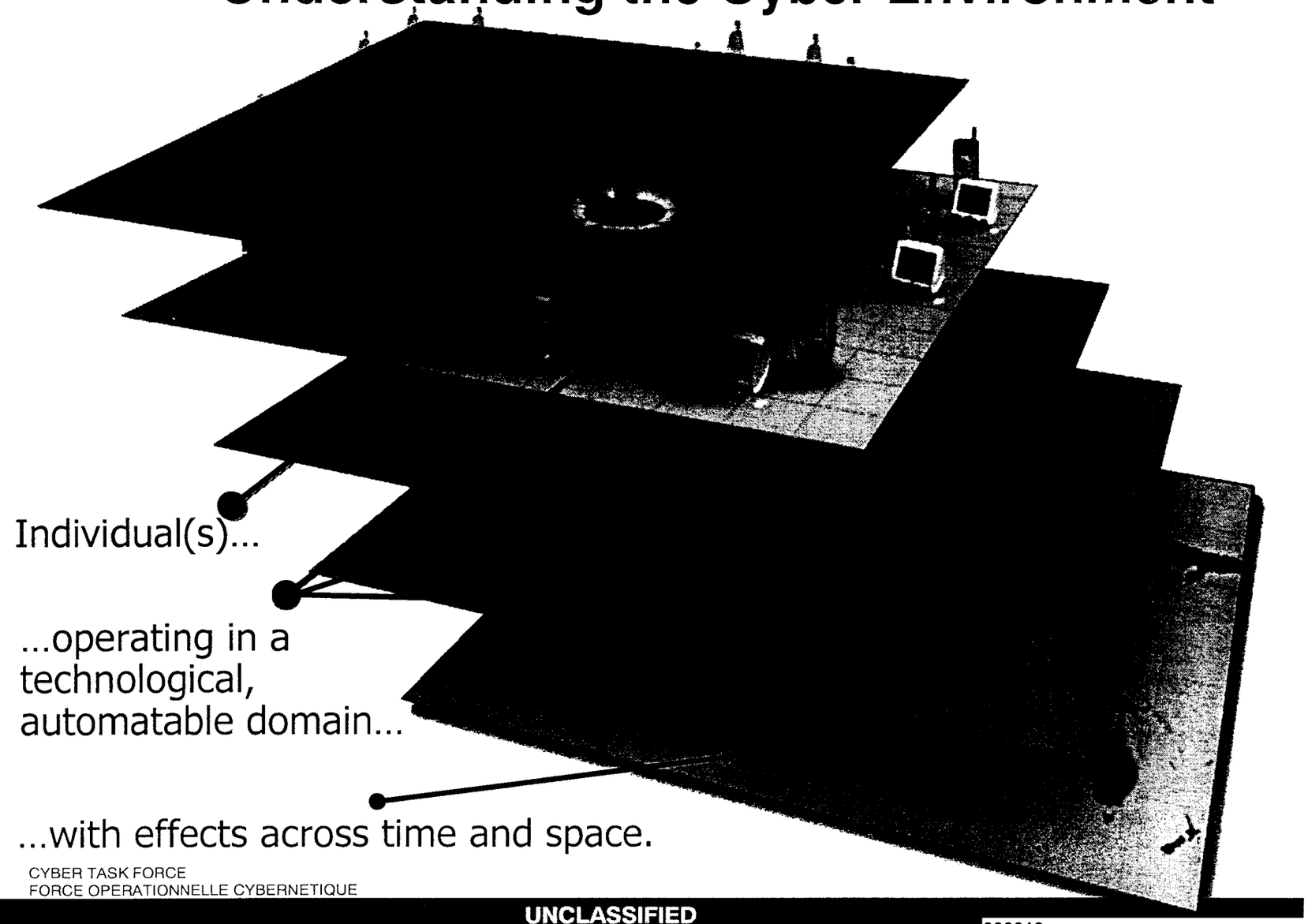
CYBER TASK FORCE
FORCE OPERATIONNELLE CYBERNETIQUE

Understanding the Cyber Environment



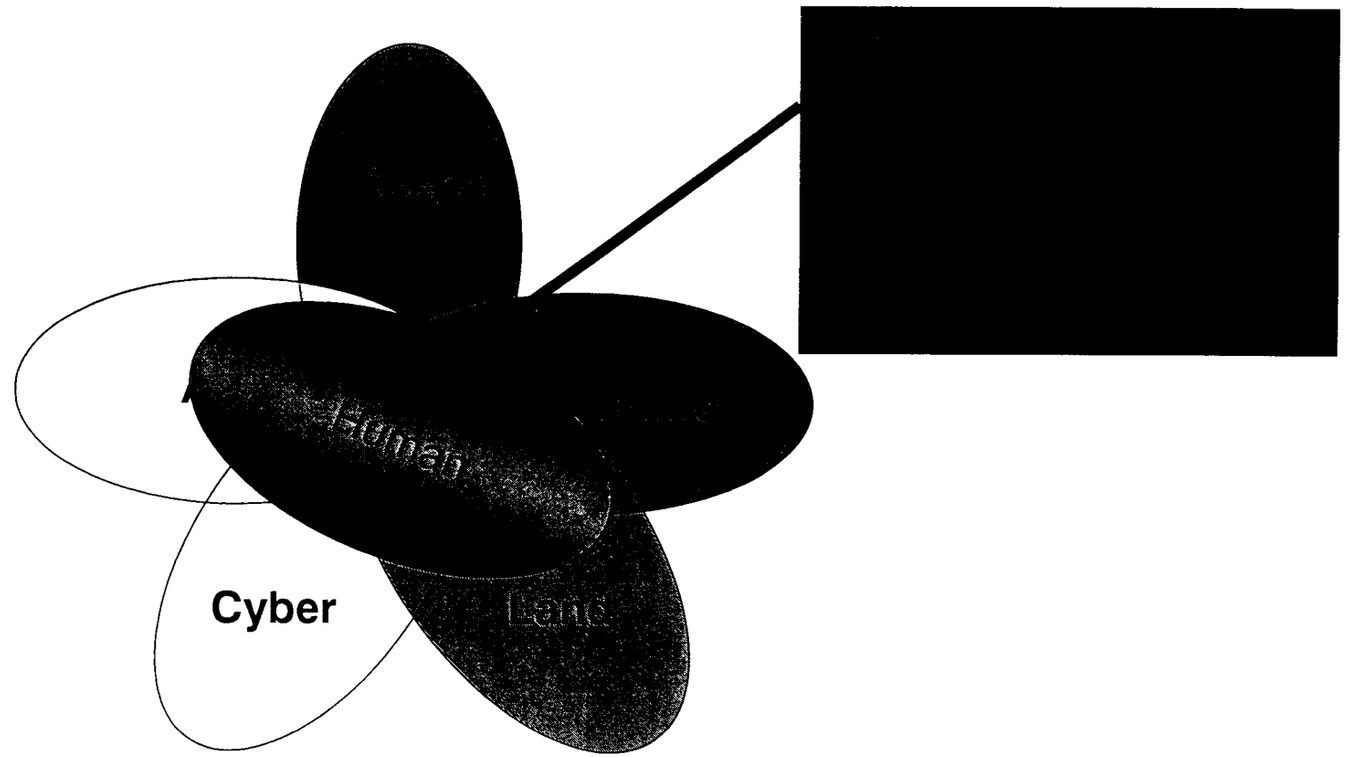
CYBER TASK FORCE
FORCE OPERATIONNELLE CYBERNETIQUE

Understanding the Cyber Environment



CYBER TASK FORCE
FORCE OPERATIONNELLE CYBERNETIQUE

Strategic Value of the Cyber environment



Two views on Cyber:

1. Cyber as an enabling capability
2. Cyber as an environment

Situation – The "As-is"

- Threat (unclassified)
  - Red Force (adversary)
    - **Capable, willing and increasingly sophisticated**
    - **Hacktivists, criminal and state sponsored**
    - **Strategic and operational objectives**
  - Blue Force (friendly force)

Situation – The "As-Is"

- Government of Canada
  - GoC Cyber Security Strategy
- Allies
  - US Cyber Command
  - AUS/UK
  - NATO
    - Coop Cyber Defence COE estb 2008 in Estonia
    - Cyber Defence Management Authority

Situation – The "As-Is"

- DND/CF
  - Framework established
    - GoC identifies Cyber as a priority
    - CFDS identifies Cyber as a threat area requiring core capabilities for the CF
    - Draft CF CNO policy
  - Cyber Task Force
    - Address lack of doctrine & dedicated resources
    - Develop top down direction that matches the bottom-up initiative
    - Seek ways to optimize current capability
    - Develop options for an improved and sustained Cyber environment competency

Modern Warspace – Changing Doctrinal Concepts

- Schriever Wargame 2010 Lessons Learned:
  - Mission Assurance is possible only through a WoG approach
  - International norms in the Cyber environment will shape plans and ability to use Space and Cyber capabilities
  - Reliance on commercial infrastructure - resilience
  - Deterrence in Cyber environments – a collective
  - Attribution problems and the ability to mask actions
  - No agreement on Signalling, Proportionality and Escalation Control
  - Decision cycles & delegating authorities: Tactical level speed of response of a Strategic capability
  - Need for ministerial level understanding of Cyber issues
  - Public-Private, Interagency & Coalition partnerships are key

Desired End State – The "To-Be"

- Comprehensive
  - Multidisciplinary approach that is inclusive of WoG, Industry, Academia and Allies
- Integrated
  - Organizational Cyber elements established (Strategic, Operational & Tactical)
  - Command responsibility to deliver cyber effects in all domains (Cyber, Land, Air, Space, Sea)
  - Integrated ops planning and force employment
- Adaptive
  - Agile, resilient, robust, flexible, creative, responsive and enduring
  - Able to meet CFDS mission requirements
  - Freedom of action for Commanders in the cyber environment
- Networked
  - Social, organizational and technology networking
  - Secure, Assured and Available

Key Linkages – The "How-To"

s.15(1)

- Joint
  - Strategic –J2 (CDI), J3 (SJS), J5 (CFD), J6 (ADM (IM))
  - Operational – Integrated into Operational Commands
  - Tactical – Integrate into extant Land, Maritime and Air domains and emerging Space domain
- Interagency
  - Partnered with CSEC
  - Governed by PSC (Cyber Security Strategy) and TBS (GC Policy on Government Security)
  - Working with CSIS, RCMP, DFAIT and other departments
- Multinational
  - Continental (NORAD/NORTHCOM)
  - Bilateral (US Cyber Command, UK GCHQ/UK Military, ADF)
  - Multilateral NATO, Coalitions)
- Public
  - ADM (S&T)/Industry Innovation
  - Academia
  - Industry partners

GoC Perspectives & Questions

- Security and Defence
  - Where they meet and how to close the gap
  - Avoiding duplication whilst improving cooperation
- Departmental Mandates
  - The attribution problem – which department is lead?
  - Impediments to Information Sharing
- Understanding through scenarios
  - Does DND have any role in the Cyber environment other than defending its own networks? Expeditionary operations? Support to Other Government Departments and Agencies? NORAD? NATO Collective Defence?
  - The Whole of Government – unexploited opportunities
- International Norms and Standards
  - Several international organizations are looking to shape the international cyber environment (e.g. NATO COE, UN, EU, OSCE, OECD, G8). What is the GoC position?

Discussion

LCol Francis Castonguay
CF Cyber Task Force

Beaudoin, Luc S.

From: - Lt
Sent: Monday, June 21, 2010 3:23 PM
To: Beaudoin, Luc S.
Cc: - Maj; - Lt
Subject:


Classification: SECRET

Good day Luc,

Here are the two reports we have produced to date on the subject incident.

Lieutenant
Advanced Analysis Team Leader
Canadian Forces Network Operations Center
Work:

Pages 24 to / à 30

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 15(1)(d)(i), 16(2)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Pages 31 to / à 62

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 15(1)(d)(i), 16(2)(c), 21(1)(a)

of the Access to Information

de la Loi sur l'accès à l'information

Moore, Bruce

From: Moore, Bruce
Sent: Tuesday, February 16, 2010 9:55 AM
To:

Cc: Williston, Sandra; Pitcher, Robert H;

Subject: CCIRC CE10-2668

Importance: High

Classification: SECRET

Good Morning All;

I believe provided a short description of this event last week. I'll provide a quick review and update with new information.

Please give me a call to arrange

Thanks very much,

Bruce Moore

Moore, Bruce

From: Moore, Bruce
Sent: February 25, 2010 8:58 AM
To:
Subject: FW: CCIRC CE10-2668

Importance: High

Good Morning

Following our earlier telephone conversation, see below the notification email I sent to

I had a follow-up telephone conversation with

Hope this helps,

Cheers,

Bruce Moore
Cyber Duty Officer
Public Safety Canada
Canadian Cyber Incident Response Centre (CCIRC) www.publicsafety.gc.ca

-----Original Message-----
From: CYBERDO
Sent: February 11, 2010 5:11 PM
To:
Cc: CYBERDO
Subject: CCIRC CE10-2668
Importance: High

Good Afternoon;

Please advise on your findings.

Thanks very much,

Bruce Moore
Cyber Duty Officer
Public Safety Canada
Canadian Cyber Incident Response Centre (CCIRC) www.publicsafety.gc.ca

Moore, Bruce

From: CYBERDO
Sent: March 12, 2010 2:57 PM
To: CYBERDO
Cc:
Subject: RE: FW: CCIRC CE10-2668

Many thanks for the update.

Do you know if is working with CFNOC on this event?

My operations manager (Luc Beaudoin) will be contacting corporate to discuss

Thanks

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From:
Sent: March 12, 2010 12:33 PM
To: CYBERDO
Cc:
Subject: Re: FW: CCIRC CE10-2668

Bruce,

This information was released to you with permission from DRDC.

Cheers.

CYBERDO wrote:
> Good Afternoon;
>
> Can you provide an update on your findings following our original notification.
>
> Thanks very much,
>
>
> Bruce Moore
> Public Safety Canada
> CCIRC
> 613-991-7792
> www.publicsafety.gc.ca

>
>
>
> -----Original Message-----
> From: CYBERDO
> Sent: February 11, 2010 5:11 PM
> To:
> Cc: CYBERDO
> Subject: CCIRC CE10-2668
> Importance: High
>
> Good Afternoon;
>

>
> Please advise on your findings.
>
>
> Thanks very much,
>
>
> Bruce Moore
> Cyber Duty Officer
> Public Safety Canada
> Canadian Cyber Incident Response Centre (CCIRC)
> www.publicsafety.gc.ca

--

Moore, Bruce

From: CYBERDO
Sent: March 15, 2010 11:17 AM
To:
Cc: CYBERDO
Subject: CCIRC CE10-2668 [New Controller]

Importance: High

Good Morning

For your situational awareness.

We've received an updated report from the department you identified in our telecon Thur 11/02/2010 4:15 PM.

Last Thursday, that department detected an internal device attempting to connect with IP (this IP was blocked after our initial report to them and this connection attempt failed). However the workstation was successful in downloading files from a different IP. (suspect this is a new controller.) The department observed files being downloaded from the following external source:

http://	images/wmcfgr.exe
http://	images/wmcsmps.dll
http://	images/fl.exe

Are you aware of any controller activity involving this IP?

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

Page 70

is withheld pursuant to section

est retenue en vertu de l'article

20(1)(b.1)

of the Access to Information

de la Loi sur l'accès à l'information

Moore, Bruce

From: Moore, Bruce
Sent: March 15, 2010 12:13 PM
To: Bastianello, Dan; CYBERDO
Subject: RE: CCIRC CE10-2668

That's all for now pending additional info from DREO. I believe I'll be requesting a CTU meeting later this week to discuss all of to CE10-2688
(I suspect there is much more that we don't know then what has been reported back to us).

Thanks,

Bruce Moore
Public Safety Canada
CCIRC
613-991-7792
www.publicsafety.gc.ca

-----Original Message-----
From: Bastianello, Dan
Sent: March 15, 2010 11:33 AM
To: CYBERDO
Cc: Moore, Bruce
Subject: CCIRC CE10-2668

Stopping.

Awaiting further instructions . . .

Dan Bastianello
Canadian Cyber Incident Response Centre
Phone/téléphone: (613) 949-8319

Email/Courriel: Dan.Bastianello@ps-sp.gc.ca
URL: http://www.ps-sp.gc.ca