# Review and Coordination of Cyber Security for Vancouver 2010

Luc Beaudoin, PEng, MSc, MBA
Chief of Cyber Operations[1]
Canadian Cyber Incident Response Centre
269 Laurier Ave W
Ottawa, Ontario, K1A 0P8
luc.beaudoin@ps-sp.gc.ca

Lynne Genik, MSc
Operational Research Scientist[2]
DRDC Centre for Security Science
222 Nepean St, 11th Floor
Ottawa, ON K1A 0K2
lynne.genik@drdc-rddc.gc.ca

## Abstract

This paper presents a review of the cyber security situation leading up to, and during, the Vancouver 2010 Olympic and Paralympic Winter Games (V2010). We narrate our experience as scientific support to the Games' Integrated Security Unit (ISU) during the final months of the planning stage, as well as during the unfolding of the Games. The events that led to our involvement, the rational of the selected approach, the key observations made during the review and the main lessons learned are described. We then present how the observations and recommendations were implemented during the Games by stakeholders such as the Canadian Cyber Incident Response Centre (CCIRC). Finally, we conclude with key recommendations intended to assist with efficient cyber security oversight of other major events, such as Olympic Games.

## 1.0 Introduction

The Vancouver 2010 Olympic and Paralympic Winter Games (V2010) were held in British Columbia in February and March of 2010. The delivery of the Games was the responsibility of a large number of organisations across private and public sectors, comprising what became known as the “three pillars” of security, public safety, and Games operations, led in BC by the Integrated Security Unit (ISU) (headed by the Royal Canadian Mounted Police), Emergency Management British Columbia (EMBC), and the Vancouver Organizing Committee for the 2010 Olympic and Paralympic Winter Games (VANOC), respectively. In support of V2010, Defence Research and Development Canada (DRDC) established a substantial project, with a primary objective of reducing the security risk through the application of science and technology. In order to help achieve this objective, scientific advisors were embedded with various organisations, including the collocated ISU and Integrated Public Safety (under EMBC). The second author was one such advisor (see footnote 2).

Cyber security had been identified as a priority area for the Games. The Government of Canada recognized the importance of information technology (IT) systems for the delivery of government services to support V2010 and a need for vigilance in the face of a growing number of cyber attacks. As a result, a V2010 Cyber Security Steering Committee was established, led by Privy Council Office, Public Safety Canada (PSC), Treasury Board of Canada Secretariat and the RCMP and, under that, a Cyber Security

[1] Formerly a system engineer with the Network Information Operations section of DRDC Ottawa
[2] DRDC Scientific Advisor to Integrated Public Safety (IPS) in British Columbia September 2008 - April 2010

Working Group (CSWG), co-chaired by PSC and the RCMP. The focus of the work was a self-assessment survey to address federal government department cyber preparedness and the cyber component of the V2010 Integrated Exercise Series (consisting of the large-scale, multi-agency Exercises Bronze, Silver, and Gold). Led by the CSWG, cyber security incidents were incorporated into Exercises Silver and Gold, though primarily contained to federal government departments due to a focus on other priorities by many of the participating organisations.

In the spring of 2009 an emergency manager with the City of Vancouver inquired about cyber threat information for the Games. At the request of Bell Canada, the Integrated Threat Assessment Centre (ITAC) had prepared an unclassified intelligence assessment outlining potential cyber threats to communications infrastructure for the Games [1]. Vancouver had this assessment as well as potentially conflicting information from past Olympics regarding cyber threats to host cities, and was looking for clarification. After inquiring with various organisations and reaching back to the DRDC network security research group, Network Information Operations, it became apparent that gaps existed in cyber threat situational awareness across government agencies and Games stakeholders. Further investigation indicated that a Games cyber threat and risk assessment including interdependencies had not been completed, though there was a misperception in some communities that the threat had been fully analysed and that some studies were larger in scope than they actually were. It also became apparent that most cyber preparations were taking place in silos, with limited integration/interaction between organisations.

The largest cyber threat to the Games may not have been loss of service through denial of service or loss of data through exfiltration, but rather impact on reputation caused by various types of hacktivism actions such as web defacements and leveraging Games infrastructure for criminal activities (bot herding, credit card theft, etc.). This is due to the international nature of the event with all eyes on Canada. Therefore, the Canada “brand”, as leveraged by VANOC and Games sponsors, was arguably the key asset to protect in cyber space. The main gap that we identified in the cyber posture was that initial efforts had not looked at cyber security from this angle. (Recently in Canada, the Treasury Board Secretariat brand protection office started to look into the cyber arena, due to cyber activity during events such as the Games and the Yes Man Environment Canada incidents in the fall of 2009[3].)

During a July 2009 meeting between the DRDC Chief Executive Officer and senior ISU staff, cyber security was identified by the ISU as a primary area of concern and, in turn, DRDC scientific services were offered. Subsequently, ISU staff were engaged to discuss a cyber security study. With their support, we proposed a project with the following tasks:

- Request a Games cyber threat and risk assessment from cyber intelligence experts and review with stakeholders to identify potential solutions and minimize risk.
- Request stakeholders to complete the Asset Management, Communications and Operations Management, and Access Control sections of the Information Security

[3] http://www.cbc.ca/canada/story/2009/12/14/hoax-copenhagen-climate.html

Management ISO/IEC 17799:2005 Audit Checklist. Verify that best practices are being applied, identify gaps and develop options for closing priority gaps.

- Identify capabilities among key stakeholders for incident response. Establish an Olympic monitoring/response capability by sharing IT service desk and network operations centre capability and contact information. Establish standard operating procedures for incident response across agencies. Establish information sharing of traffic monitoring at stakeholder gateways in advance of the Games to pick up reconnaissance attempts or emerging threats.
- Review information exchange requirements already captured and how they are to be fulfilled, identify Internet service provider (ISP) critical dependencies.

Admittedly, it was a late start to the project. However, at that time network architectures for some of the new organisations were still under development and/or not fully deployed.

This paper recounts our subsequent experience in attempting to carry out these tasks, outlines what was accomplished along with observations and lessons learned, and includes recommendations for future major events.

## 2.0 The V2010 Planning Phase

### 2.1 Approach

In order to carry out the cyber review, a small team was formed, consisting of the DRDC Scientific Advisor to IPS and a research engineer from DRDC Ottawa Network Information Operations (the authors), a member of Department of National Defence (DND) Chief of Defence Intelligence Computer Network Operations, the security representative of the ISU Informatics team, and, initially, a member of the Canadian Security Intelligence Service (CSIS). The team was split between Richmond, BC and Ottawa, ON.

Figure 1 shows a connectivity schematic for V2010 that was developed by IPS (note that the links indicated are for information sharing or authority, rather than network connectivity), which provided a starting point for defining the problem space. The figure is shown here to depict the scope of the problem rather than to define the various organisations. The public safety pillar is denoted in blue, the Games operations pillar in pink, and the security pillar in yellow. Given time and resource constraints, Figure 1 was instrumental in focussing our efforts. We made the assumption that each organisation had applied network security best practices within their own boundaries and, therefore, that key remaining cyber risks resided at interconnection points. We took a top-down approach to service prioritization, starting at the top with VANOC as the face of the Games for Canada. From this point, we included the ISU/RCMP and DND as key federal security groups. It was also clear that the provincial and municipal levels should be considered because of their mandates related to emergency response and relationships with first responders and critical infrastructure resource owners/operators. This seemed, however, to explode the scope of our study. We decided to focus our efforts at the provincial level on the Shared Services BC (SSBC) organisation, which provides IT

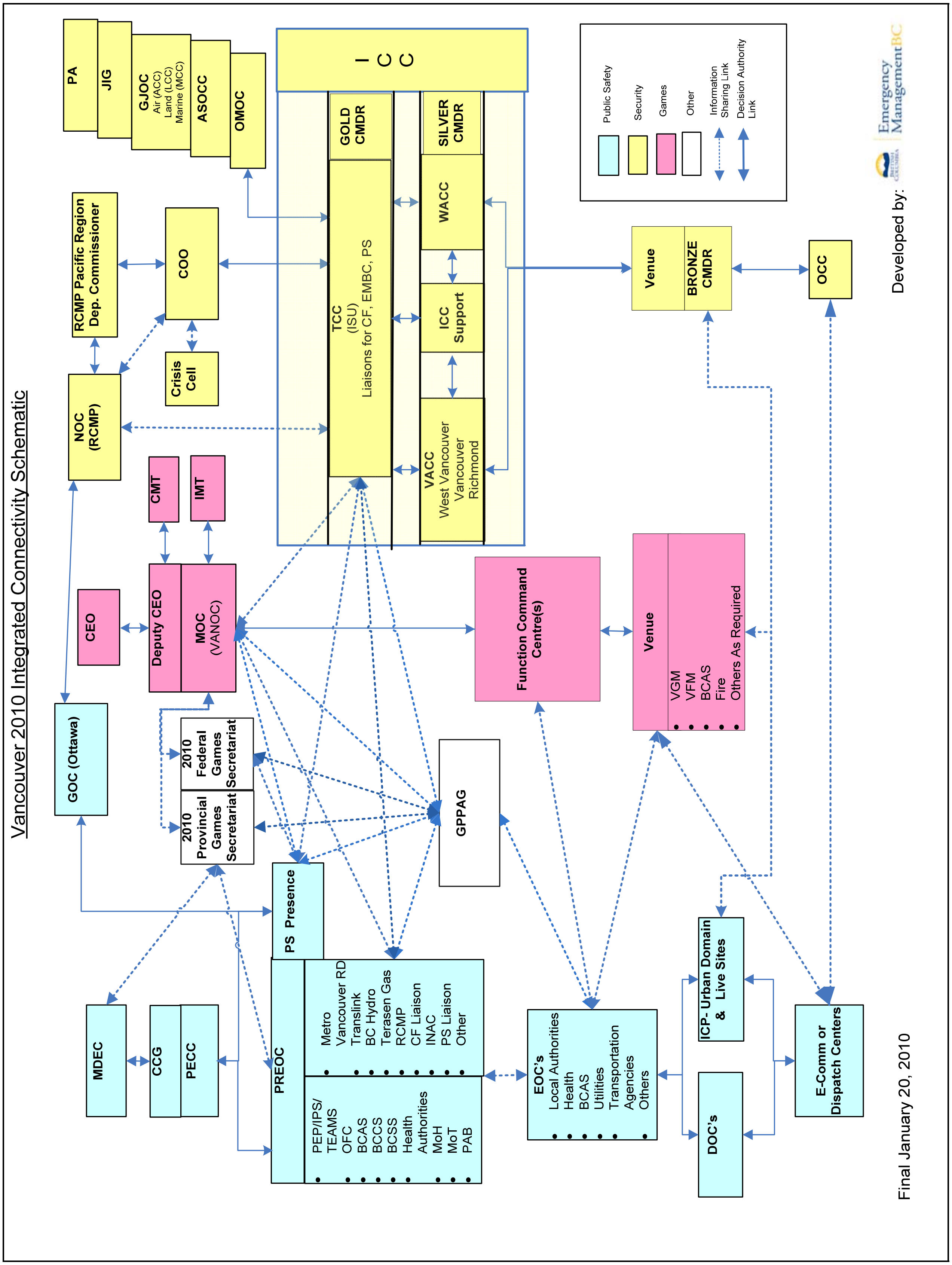

Figure 1. Vancouver 2010 Integrated Connectivity Schematic (courtesy EMBC)

infrastructure support services for the BC government, such as connectivity, service desk, web presence, and security. For the regional level, an organisation called E-Comm seemed like a promising starting point. E-Comm provides a 911 call centre, dispatch services for a number of police and fire departments in the Vancouver area, and an interoperable first responder radio system. We also consulted with Bell, the official network provider of the Games, and ISP to both VANOC and the ISU. We leveraged trusted, often personal, relationships and contacts to obtain buy-in from these organisations, which was critical since participation was voluntarily. The ISO Audit Checklist, an existing standard, was distributed with a request to complete the sections mentioned earlier.

The intent was to use the ISO checklist to gather data to develop a baseline understanding of the situation; however, responses were not received in the timeframe requested. Probing indicated that time and resources were short, so a new approach was taken. Face-to-face meetings were held with each organisation (with the exception of the province, which was done by conference call) to address the following questions:

1. Background knowledge: What are your critical tasks/mission areas?
2. What do you perceive as your most critical IT assets, services and information?
3. Configuration management: What topology and host configuration information do you have?
4. Access control: How are physical and network access managed?
5. Network management: How are monitoring of hosts and links performed, and by whom?
6. Vulnerability management: Do you monitor vulnerability releases, or regularly scan your assets? What is your patch management process?
7. Host security: What virus scanner, host intrusion prevention system, vulnerability scanner, etc. do you use? How are these tools managed and updated?
8. Network zoning (firewalls, gateways, access control lists): Provide an overview. How they are managed, and by whom?
9. Do you have a network operations centre, computer emergency response team, help desk (for points of contact)?
10. Do you review logs and/or intrusion detection system alerts?
11. What is the network geographic and physical deployment?
12. What are the relationships with ISPs and vendors (Bell, Telus, etc.)?
13. Do you have a recent TRA?
14. How would you manage a cyber incident, accidental or malicious? (Communication details with ISU, ISPs, others.)
15. Do you have cyber security concerns you would need us to look at?

The subject matter experts and the level of information provided varied by organisation. For example, the VANOC Director of IT Operations, Security & Technical Operations Centre and IT Security Manager spent a significant amount of time with the team (on the order of a couple of days) to discuss the above questions, while interactions with another organisation consisted of several short meetings with IT staff followed up with email to gather information.

## 2.2 Observations

As contextual information was collected by interviews, the following observations became increasingly evident:

- The priorities of organisations varied according to their mandate and structure. For example, VANOC's "Games" network, hosting critical information such as time and scoring results, took priority over their other networks, such as the "Admin" network. Alternately, the provincial network/security groups were viewing the Olympics more or less as "business as usual". For Bell and VANOC, the ISU may have been important, but by far NBC, with their approximately $1 billion purchase of broadcasting rights and communication requirements to support that, clearly outweighed every federal, provincial and municipal organisation.
- A common concern raised by stakeholders was the lack of (actionable) cyber threat intelligence information. This problem is not unique to the cyber domain. On the one hand, intelligence agencies need to declassify/compose information in such a way that it gets to the right communities. On the other hand, there may be a misperception about the type of cyber threat intelligence information available. For one thing, attackers generally do not publicize their intent for an imminent attack and, in most cases, prefer to remain undetected. As a result, intelligence available is largely focussed on technical capabilities in general and based on historical observations. The technical capabilities are rarely fundamentally new due to the large amount of exploitable vulnerabilities in most IT infrastructure and past events do not speak to the likely target or time of the next attack; however, they do speak to the technology involved, which, as just mentioned, is not novel in most cases. Noted techniques include traditional phishing attacks on key organisations supporting the event, search engine optimization leveraging event themes, web defacements or copy, and denial of services using botnet infrastructure.
- No single organisation had overall awareness of the telecommunication assets supporting the Games and their interdependencies. This was evidenced by the fact that no single ISP supported all organisations: VANOC was with Bell, DND with Telus, ISU with Bell/VANOC, provincial and municipal organisations were with a mix of local and national ISPs, and many federal departments had individual contracts with ISPs like Bell and Telus, the two main service providers of the region. This implied the need for a consultative approach to managing potential incidents.
- The density of telecommunication assets was extremely high .This included both physical and spectrum density. This implied that even relatively small cyber incidents could affect many stakeholders.
- Most organisations shared some critical IT assets, such as fibre links, hosting facilities, cyber security response capabilities, contractors and service providers, sometimes without an awareness of a shared dependency. Examples of this are as follows:

a) Some of the IT backbone infrastructure included fibre links owned by the City of Vancouver, but managed by E-Comm;
b) Some of the ISU IT services were provided by VANOC, some others by E-Comm, and VANOC physical security (including server rooms) was managed by the ISU, despite the fact that all these organisations had other mandated priorities (ISU securing the Games, VANOC delivering the Games, and E-Comm providing 911 services, dispatching first responders, and management of a first responder radio system);
c) The fibre infrastructure of the region had been significantly affected by recent events such as landslides and accidental cuts.

This implied that potential cyber incidents requiring restoration prioritization may need a third party broker to ensure the service owner considered national interests, such as citizens' safety, over existing service level agreements.

- The combination of density and interdependencies made some important assets for individual organisations become holistically critical for the Games. This implied that additional security features may be warranted, such as redundancies and access controls, or at least awareness of these assets for incident mitigation coordination. The main VANOC server room, key fibres and third party hosting facilities were such assets.
- There was no system, authority or forum for deconflicting potential issues such as restoration priorities and resource coordination, specifically for shared assets.

Given the scarce remaining time available, we focussed efforts on the processes for information sharing and coordination of cyber security incident prevention and resolution between partners.

### 2.3 Lessons Learned

Lessons learned throughout the information gathering exercise include:

- Establishing trust and credibility is critical. Face-to-face discussions are most effective for this purpose. Organisations participated in the review voluntarily and decided the degree to which they would share information. When there is no mandate to share, the importance of relationship-building and trust cannot be underestimated.
- Access to the right subject matter experts (SMEs) is key. Spending a small amount of time with SMEs can yield a great amount of credible information. However, not having access to the right experts can result in incorrect information and/or a requirement to follow up on and validate information provided.
- Not all levels of government (municipal, provincial, federal) have a computer emergency response team capability. This made finding the key cyber security contacts more challenging since we weren't able to tap into pre-established communities/contacts.
- The degree of buy-in varied. Organisations were preparing until the very last minute and those that were further along in their planning generally had more resource availability for this activity.
- Despite organisations working closely together, the value of information sharing in the cyber domain was not recognized by many organisations from the onset.

- The ISO checklist proved to be too formal and overwhelming to collect contextual information. Focussing on a shorter and simpler list allowed for engaging with technical staff to obtain valuable contextual information which would not have been obtained otherwise.
- For the most part, threat and risk assessments had not been formally completed by key organisations for the Games. This was partly explained by some stakeholders' IT infrastructure not being completed until a few weeks before the event. As a result, cyber security knowledge remained largely in a tacit form with IT specialists, which the interviews were able to make explicit.

Upon completion of our review, we provided a summary and recommendations to the ISU, and engaged the Canadian Computer Incident Response Centre (CCIRC) for the operational period.

## 3.0 V2010 Games Operations

### 3.1 Approach

In order to increase situational awareness during the Games, we produced a list of key technical stakeholders and proposed an incident reporting structure. The stakeholders were chosen for their ability to control cyber resources. Prior to our review, the assumption for managing cyber security events was that reporting would occur following the same channels as physical events such as bombs, riots and plane crashes. Current provincial and federal plans do not recognize that building a trusted cyber community and dedicated technical communication channels is paramount for emergency management involving cyber incidents. However, we assert that it is necessary for the following reasons:

1. Every organisation owns a piece of the cyber security puzzle. There is no lead federal department mandated for major event (such as the Games) cyber oversight, holistically, unlike other security and emergency management areas such as health and physical security.
2. Since cyber incidents often involve embarrassing consequences, such as data exfiltration, reporting is unlikely unless trust exists a priori.
3. The technical and complex nature of cyber events, as well as the specific terminology used, requires that information be obtained as close as possible to the source to maximize accuracy.

We proposed that the CCIRC be the national organisation leveraged for fostering the Games cyber community and information sharing. The reporting structure amongst community members leveraged existing federal structure while maximizing lateral exchanges. The chart shown in Figure 2 presents the key Games stakeholder community and their formal communication channels. We proposed that CCIRC host a periodic teleconference with these stakeholders during the Games to facilitate information exchanges and build trust. These teleconferences were put in place a few weeks before the Games, hosted every second day to limit their impact on operations, and lasted on average 15 minutes.

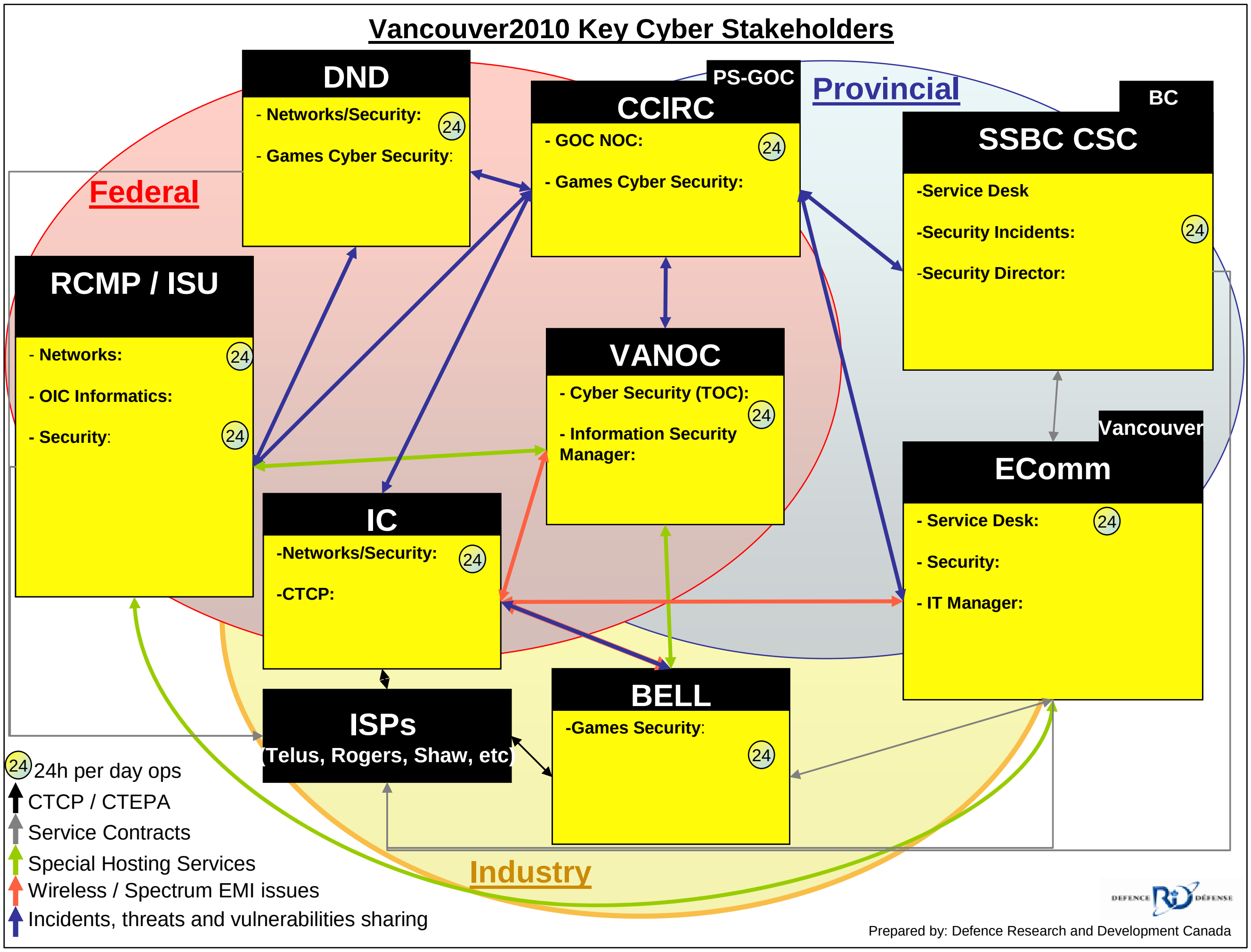

Figure 2. Vancouver 2010 Key Cyber Stakeholders

## 3.2 Observations

VANOC was a target for malicious cyber activity during the Games. The following cyber activity occurred during the Olympics and was shared in the stakeholder forum:

- A copy of VANOC’s web site, hosted in the Ukraine, leveraged interest in the luge accident to distribute a fake video CODEC malware. VANOC and CCIRC collaborated to identify and take down the perpetrating Ukrainian site.
- Search engine optimization (SEO) poisoning with Olympics themes was used to distribute malware/crimeware. VANOC identified this activity, resulting in a CCIRC cyber security awareness bulletin.[4]
- Minor virus infections were reported and handled locally, but shared amongst stakeholders. Support was offered across organizations if required.

[4] http://www.publicsafety.gc.ca/prg/em/ccirc/2010/in10-001-eng.aspx

- There was rapid deconfliction of “cyber attack” reports, such as misinterpretation of the SEO poisoning events as actual attacks on the Games IT infrastructure.

Although the initial group invited to join was limited to key stakeholders, it quickly grew to include a number of liaison officers and representative from central agencies. The stakeholder community decided to continue the CCIRC-led conference calls into the Paralympics (at a decreased frequency). There was very little activity to report during the Paralympics.

### 3.3 Lessons Learned

The conference calls hosted by CCIRC became the defacto cyber forum during the Games, and as a result, attendance grew. Participants increasingly leveraged the forum for sharing information as trust was built and collaboration occurred, which happened early on as a result of the Ukrainian copy of VANOC’s web site. The community was also leveraged outside of the teleconference to pass information, particularly to the broader emergency response community to clarify reports of cyber attacks.

The frequency and the format of the conference call required minimal resourcing. This was certainly an important factor in its success – keeping the call short and to the point made it an efficient use of time.

Secure information sharing mechanisms were also made available to the stakeholders before the Games start. These included PGP and PKI keys for emails. Although not used for most of the information exchanges, these mechanisms helped in building trust amongst stakeholders by providing some level of comfort around data protection.

Finally, a close relationship between CCIRC and Industry Canada (IC) allowed leveraging of the Canadian Telecommunication Cyber Protection (CTCP) forum where most Canadian service providers were represented. This relationship also brought together both wireless/spectrum incident capability management, housed within IC, and cyber incident coordination capabilities, housed at CCIRC.

## 4.0 Conclusion

V2010 was a major event with an abundance of private and public sector organisations working together to ensure a safe and secure Games. Cyber due diligence from a holistic perspective was necessary to protect Canada’s brand, and we recognized a lack of this activity as a gap in the lead up to the Games. With the support of the ISU, we formed a small team of four to five people (roughly one full-time equivalent) and, over the course of the subsequent six months, performed a cyber security review of key stakeholders and built a Games cyber security community. While this was seemingly done in the eleventh hour, in retrospect it may not have been possible to complete some of the tasks earlier due to the evolving network architectures and plans of key participating organisations, as well as challenges in identifying critical people.

Future major events will likely be subject to the same the issues we identified for V2010, namely an interconnectedness and reliance on the same critical IT assets and/or service providers by multiple stakeholders and conflicting organisational priorities. Given that stakeholders span public and private sectors and that prioritization of service restoration and coordination of resources may be required from a national perspective during a significant cyber event, there is a need for a national organisation to build trusted relationships with public and private sector partners, provide cyber due diligence by working with partners to identify and mitigate gaps, and provide leadership and prioritization for response.

Our experience has shown that formalizing a cyber security community, composed of the key cyber stakeholders, through face-to-face meetings and frequent, but concise, teleconferences, increased shared understanding of the context, created trust between stakeholders, enabled information sharing and improved efficiency in incident response coordination. Furthermore, this was done in a resource-efficient manner. Attaining overall situational awareness upfront may have been too much to hope for, but having the technical forum for information sharing may have been the next best thing.

## References

[1] 2010 Vancouver Winter Olympics: Security Threats to Communications Infrastructure, Integrated Threat Assessment Centre Intelligence Assessment, September 22, 2008, Unclassified - For Official Use Only