13th ICCRTS: C2 for Complex Endeavors

"Coalition Computer Network Defence (CND) Common Operating Picture (COP) Concept"

Topics: C2 Concepts, Theory, and Policy; Multinational Endeavors; Networks and Networking

Lynne Genik
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, ON K1A 0Z4
lynne.genik@drdc-rddc.gc.ca
Tel: 613-993-9942
Fax: 613-993-9940

Julie H. Lefebvre
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, ON K1A 0Z4
julie.lefebvre@drdc-rddc.gc.ca

Mike Froh
RatworX Inc.
1138 Hartwell Road
Ottawa, ON K4M 1E5
mike@ratworx.com

POC: Lynne Genik

Coalition Computer Network Defence (CND) Common Operating Picture (COP) Concept

Lynne Genik, Julie H. Lefebvre, Mike Froh
Defence R&D Canada

Abstract

This paper defines a conceptual Coalition Computer Network Defence (CND) Common Operating Picture (COP), its concept of operations, and identifies research challenges for providing such a capability. A Coalition CND COP consists of two aspects of information assurance (IA) in a coalition environment: technologies for secure information exchange and the automated exchange of multinational CND information; this paper focuses on the latter. Situational awareness (SA) is a vital part of CND, providing an understanding of the status of networks. CND SA encompasses IA information including available information technology (IT) services, IT infrastructure, vulnerabilities, safeguards, exploits, threats, alarms, and incidents. All of this information can contribute to a Coalition CND COP. We identify four reasons for automating the information exchange: human resistance to sharing, rapid events, a large information exchange volume, and information complexity. Scenarios involving a Coalition CND COP are presented to illustrate improved operational capabilities, including clearer SA, more efficient use of resources, and more effective CND action. It is shown that even a small amount of information sharing can have significant benefits. Finally, a number of research areas supporting a Coalition CND COP capability are detailed and prioritized.

Keywords: common operating picture, information assurance, computer network defence, network situational awareness, coalition operations, network command and control, CND COP

1. Introduction

Militaries are heavily reliant on communication networks and are becoming increasingly so with the move towards network-enabled operations. Both the networks and the information carried on them must be safeguarded. Regardless of the efficiency of the safeguards, events will nevertheless occur (such as equipment malfunctions, malicious attacks, maintenance, etc.) that can negatively affect operations. Information assurance (IA) and computer network defence (CND) provide a means to protect and defend information systems and computer networks. Situational awareness (SA) is an essential part of CND since it provides an understanding of the status of networks, including the impact of various events on the network and the risk to operations [1]. To provide CND SA for coalition operations, it is beneficial for coalition partners to share CND information. A Coalition Computer Network Defence (CND) Common Operating Picture (COP) is a means of sharing, assessing, and displaying relevant information across coalition boundaries so that it may be easily accessed and quickly understood. In this

paper we define concepts for a Coalition CND COP, propose a concept of operations, and identify and prioritize areas requiring research.

While COPs exist to provide SA for the land, air, sea, and joint environments, they are only now under development for the network realm. Nations, such as Canada with its Joint Network Defence and Management System (JNDMS) [2], are developing CND COPs. Computer networks are unique in that they are both an enabler in enhancing conventional physical battle and an environment unto themselves in which to conduct information warfare. Thus, CND COPs will support national networks but will also need to be linked to COPs supporting operations since network events may affect other environments. Accordingly, a CND COP is not meant to operate in isolation but is intended to be part of a larger command and control (C2) system.

Beyond operating in national environments, C2 systems must be able to interoperate with other nations for coalition forces to operate effectively. For the Canadian Forces (CF), coalition operations have been identified as a necessity in Canada's international policy, which states: "No state, no matter how powerful, can, by acting alone, make itself invulnerable. In an interconnected world, countries find themselves sharing mutual interest more often than ever before." [3]. The Multilateral Interoperability Programme (MIP) is an example of an extensive, international endeavor to develop interoperable specifications for C2 information sharing to improve SA. Similarly, coalition CND information sharing will require mechanisms for information exchange, and these can be defined using a Coalition CND COP.

Multinational IA information sharing exists today between some nations, but in relatively simple forms such as by phone, email, or through web portals. The Internet Storm Center [4], run by the SANS Institute, is well-known for providing a global view of malicious Internet activity. It provides warning and analysis services through its distributed intrusion detection system, which is based on user log submissions. Intrusion detection has been the focus of research and development efforts for multinational IA information sharing to date. Germany's Forschungsgesellschaft für Angewandte Naturwissenschaften investigated a cooperative multi-domain intrusion warning system [5, 6] and the Internet Engineering Task Force Intrusion Detection Working Group defined an intrusion detection message exchange format [7] and exchange protocol [8]. The concept of a Coalition IA COP (CIA COP) has been explored previously, including through a United States (U.S.) led CIA COP Advanced Concept Technology Demonstration [9], with a focus on intrusion detection information sharing. Recently the North Atlantic Treaty Organisation's (NATO) Research and Technology Organization (RTO) Information Systems Technology (IST) Panel formed a technical team, NATO IST-081, "Coalition Network Defence Common Operational Picture", scheduled to begin work in 2008.

We develop the concepts for a Coalition CND COP in this paper. A Coalition CND COP consists of two aspects of IA in a coalition environment: (1) technologies and architectures that allow coalition members to securely exchange information (common to all COPs) and (2) multinational CND information sharing. We focus on the latter, on automating the information exchange and the associated challenges in particular. Reasons to automate the exchange are introduced in Section 2 and the Coalition CND COP vision

is presented in Section 3. We explore several operational scenarios to demonstrate the types of circumstances in which a Coalition CND COP is advantageous in Section 4 and discuss the overall benefits in Section 5. Research gaps related to multinational CND information sharing in a Coalition CND COP are identified and prioritized in Section 6, followed by the conclusion.

2. Motivation for an Automated Coalition CND COP

The justification for adopting any COP is based on the principles of war (such as security, flexibility, concentration of force, maneuverability, etc.) with the intended outcome that your Observe, Orient, Decide, Act (OODA) loop is quicker than your adversary's. A Coalition CND COP should serve to enhance the information available in the IA OODA loop among coalition partners. Nations share IA information when they have shared network resources, shared operations, or as a "for your information" only. In general, the information exchanged can relate to all phases of the OODA loop (for example, sharing sensor information, sharing fused data, sharing courses of action (COA), and acting on the chosen COA).

An assessment of the current mode of operation revealed that, at least from a Canadian perspective, there is always a person involved in multinational IA information exchange. A human typically decides what information is shared and when, and the processes for doing so are predominantly manual in nature. We propose the following reasons to automate IA information sharing:

1. Human resistance to sharing. Having humans decide when (or if) to share information in a coalition can result in resistance to information sharing. This means that pertinent information may not be shared or there may be delays in information dissemination, impacting its usefulness. The resistance to share might be based on operators being too busy, no perceived benefit to sharing, lack of trust of coalition members, unclear policy on when to share, or sharing being a lower priority task, for example. Establishing automated sharing mechanisms forces militaries to clearly articulate the criteria that warrant information sharing in advance, rather than leaving it to the judgment of individuals. Recent observations by coalition forces in Iraq note, "Officials from coalition countries, speaking at the conference, said a lack of trust, not technology, is the primary stumbling block to information sharing. … Future multinational information sharing will be identity-based, based on information assurance architecture. 'We'll let the software decide who gets what.'" [10].

2. Rapid event time scales. Militaries have been adapting to increased battle tempo for many years. The network tempo, in particular, is exceedingly fast. IA events such as worm or Trojan horse propagation can occur with such great speed that automated detection and information sharing becomes the only effective way to deal with these types of events. The 2003 Slammer worm is a well-known example of the speed of propagation and the resulting havoc. It reached its full scanning rate of more than 55 million scans per second in roughly 3 minutes and compromised over 90% of vulnerable hosts worldwide in less than 10 minutes [11].

3. Information exchange volume. In IA space, raw or partially processed network sensing information can constitute huge volumes of information, exceeding the capacity of manual methods for processing the information. In the network security world this is a big problem and is being tackled by some commercial products, such as Intellitactics [12], ArcSight [13], and nFX One [14], that automate tasks for monitoring, alerting and managing incidents.

4. Information complexity. Information complexity can occur in all phases of the OODA loop, including the fusion of complex sensor information and taking IA action. Fusing sensor data may require the analysis, filtering, and correlation of data from many potentially disparate sources; for example, data collection and analysis may occur in different time zones, hosts could be running any combination of the thousands of available commercial-off-the-shelf software products, network topology and systemic dependencies can make information difficult to present in simple forms, SYSLOG servers may collect hundreds of thousands of events per day, of which any subset may need to be correlated to past or future events, etc.

MIP's role of providing uninterrupted support to command and control alludes to the same reasons for change [15]:

Digitisation of C2 information seeks to facilitate increased operational tempo by reducing the need to slow down, or stop, in order to regain situational understanding. In order to realise this operational objective, information must continue to flow as the forces move throughout the battlespace. Since commanders may need to receive and disseminate situational awareness and execution information from any location in the area of operations, all of the sources and destinations of information should remain available to the commander at all times. Interoperability seeks to remove C2IS boundaries as a barrier to the timely flow of accurate and relevant information between commanders and staffs within a multinational force.

3. Coalition CND COP Vision

As stated earlier, a CND COP is intended to be integrated into the larger C2 system. The same is true of a Coalition CND COP; it is envisioned to be part of both the national COP and the overall Coalition COP. We assume that nations will share CND information through a Coalition CND COP, ideally using their CND COPs. This concept is illustrated in Figure 1.

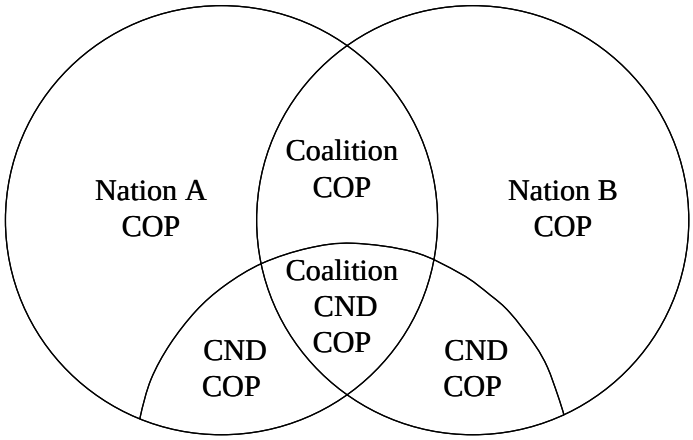

Figure 1. A Coalition CND COP is envisioned to be a subset of a Coalition COP and national COPs

The notion of a COP that we support is defined by the NATO IST-036/RWS-006 Working Group 1 [16]:

The "Common Operational Picture" refers to the vision the different collaborating parties have of the state of an operation. It is "common" insofar as the relevant data about each other's goals and capabilities, as well as about the external situation, is available to all parties. It is "operational" to the extent that the data are available at the time they are needed, in a form useful to the parties. It is a "picture" to the extent that it allows the parties to form their own mental image of the situation in which they are operating. A true "Common Operating Picture" emerges, not when the parties have the same picture, but when their different viewpoints on the situation allow them to cooperate without misunderstandings of their respective roles and functions within the operation. This happy condition may or may not come to pass when the parties see the same display, but it cannot come to pass unless they have shared access to the relevant data.

Thus, we do not envision a Coalition CND COP to necessarily consist of a single identical display of information, but rather that the relevant information is available to all parties involved and displayed as each sees fit. The information shared is not limited to intrusion detection information but includes all CND information such as information technology (IT) services, IT infrastructure, vulnerabilities, safeguards, exploits, threats, alarms, and incidents [1]. However, at this point we do not define specific data elements that must be shared to provide increased coalition CND SA. Beaudoin et al. define information requirements for CND SA from a top-down approach, which involves the amalgamation of network management and network security. The model provides a road map for the fusion process that needs to take place in order to answer the following types of questions that the network commander may need to answer, including [1]:

- What is the network mission?
- What are the mission critical resources?

- What is my defensive posture?
- What is happening? Am I under attack?
- What is the current threat level?
- What is the level of risk to my network mission?
- What is the impact to my network mission?

It is assumed that nations will retain control over the CND information they share in a coalition for sovereignty and national security reasons. The overall architecture to achieve a Coalition CND COP must allow this autonomy. MIP employs this architectural approach with each nation having autonomous C2IS systems that share C2 information with the coalition according to their national policies. We envision that the Coalition CND COP information exchange will eventually become a subset of C2 information exchange, such as MIP[1].

Figure 2 shows the idealized Coalition CND COP architecture where each nation has its own C2 COP, which includes a CND COP. The C2 COP and the CND COP both receive environmental inputs from a number of sensors, which are analyzed to provide national SA. A guard function provides the interconnection to the coalition and maintains the national policy on coalition information sharing. The coalition wide area network (WAN) provides the interconnection path among the cooperating nations and is an amalgamation of networks owned by coalition members (it is assumed that each member is responsible for, and willing to maintain, their portion of the network). This ideal connectivity could be achieved using physically secured local area network connections or could involve distributed virtual private network (VPN) connectivity using encryption devices. A Policy Based Network Management [17] capability would allow the establishment of secure communication between authorized coalition networking entities. The double-headed arrows within the coalition WAN in Figure 2 represent bilateral Coalition CND COP information exchange agreements. It is difficult to illustrate the Coalition COP itself and the Coalition CND COP within it; they are effectively defined by the double-headed arrows and the information exchanged through the bilateral agreements.

The architecture must be capable of handling bilaterally negotiated information exchanges in order to model complex dynamic coalitions. For example, nations A, B, and C may be participating in a joint exercise at the same time as nations A and B are holding a separate exercise. Additionally, complex coalition operations may involve many partners who are involved in the joint action but not equal coalition partners; therefore, the ability to bilaterally control Coalition CND COP information flow within the coalition is required.

---

[1] We believe it is important to draw upon C2 research and development for parallels/application in the network world.

Communities of interest should be established using caveat/category separation on national networks to facilitate coalition information sharing using a suitable technology, such as content-based separation (for example, Canada's Secure Access Management for Secret Operational Networks (SAMSON) [18]) or network level separation (for example, using NetTop [19, 20] to host various virtual machine instances on a single machine). Nations should support the capability to control user access to coalition information by checking their credentials and limiting access to information based on the user's authorization. In addition, the information should be securely labelled for release to coalition members and formatted in a CND data model so that it can be automatically exchanged. The information labels will need to include classification as well as release labels.

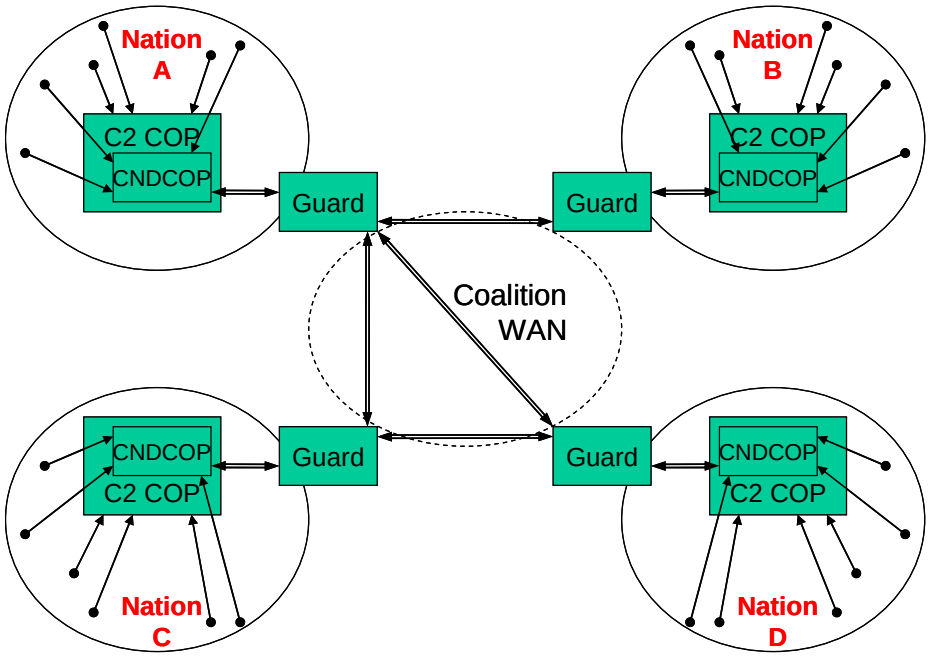

Figure 2. The Coalition CND COP Architecture

While an automated Coalition CND COP will ultimately result in fewer human resources, militaries may need CND analysts in the field to deal with the increased amount of CND SA information being shared. Typical deployments in a coalition will have limited backhaul bandwidth from the coalition location to national IT infrastructures. As such, it is not practical to backhaul the anticipated volume of exchanged information in a timely fashion and the pace of events will require that analysts are able to respond immediately, particularly when it comes to cyber operations.

4. Operational Scenarios

Three operational scenarios are presented in this section to illustrate how a Coalition CND COP could be used. They were developed to demonstrate the various reasons to automate as summarized in the following table:

Scenario	Reason to Automate			
	Human Resistance	Rapid Event	Info Volume	Info Complexity
Strategic Alliance – NVAT Cooperation	✓			
Deployed Theatre Operations – Shared IDS Data		✓		
Deployed Theatre Operations – VM Migration			✓	✓

Table 1. Coalition CND COP Scenario Reasons to Automate

4.1 Strategic Alliance – National Vulnerability Assessment Team (NVAT) Cooperation

In this scenario, the various nations share human resources to deal with a new vulnerability. The triggering incident occurs during normal working hours in Nations A and B, which have fully manned operations centres, and during night hours in Nation C, which has a blacked out operations centre with on-call personnel. The situation can be handled by the current methods used to share IA information involving a human in the loop, such as phone, email, etc.; however, we explore the use of a Coalition CND COP and discuss its utility. We assume that all nations share a watch list of used applications, and that there exist strong pre-established information sharing relationships.

Flow of events

1. A new buffer overflow vulnerability in Vendor X type firewalls is released through Mitre's Common Vulnerability and Exposures website. The vulnerability can lead to a denial-of-service of firewall services and may ultimately expose networks.

2. A notification is automatically produced through the national CND COPs and each nation begins to assess the potential operational impact on their network. Since a watch list of IT applications is shared through the Coalition CND COP, nations aware that the firewall is deployed in each country.

a. Nations A and B CND COPs produce notifications at watch desks and, since it is normal working hours, each national operations centre starts acting on the new information. Nation A is using the vendor's firewall to separate internal enclaves that are not connected directly to the Internet so not at immediate risk; however, Nation B's CND COP indicates high risk since this type of firewall protects their military networks from

the Internet. The severity of this vulnerability with respect to each nation is automatically shared through the Coalition CND COP.

b. It is night hours for Nation C and on-call duty personnel are notified. They evaluate the situation (for example, using remote access to their CND COP) and notice there is also a high risk to their networks. They see, through the Coalition CND COP, that Nation B is in the same situation. Rather than waking other staff, Nation C contacts Nation B to work on the problem with them.

3. Nations B and C request that Nation A focuses intelligence gathering on exploits from hacker groups for the new vulnerability. Sources indicate that there may be a potential exploit within two days, increasing the risk to Nation B and C networks. This threat information is automatically shared through the Coalition CND COP.

4. Nations B and C independently choose COAs that minimize impact to their national operations. Countries begin developing workarounds based on their security architecture. Generic information about how to handle the vulnerability is shared.

5. Nation B develops an IDS signature to detect exploit attempts until a patch is developed and rolled-out, which they share with the other nations through the Coalition CND COP.

6. Vendor X releases a patch for the vulnerability. Nation C tests the patch in their lab during the night to identify and address issues with implementation, which allows all nations to deploy the patch with minimum risk.

Discussion

While this scenario is fairly straight-forward, it demonstrates that sharing information as simple as a watch list of applications within the coalition has benefits. Under different circumstances it may be beneficial for the nations to share more details, such as a filtered view of their respective network infrastructures; for example, if assets are shared within the coalition it might be useful to see how the shared resources are connected to each nation's infrastructure to assess exposure. Automatically sharing both the watch list and the threat information results in clearer coalition SA. A second benefit of this scenario is the efficient use of coalition resources; Nation A focuses on data mining hacker sites, Nation B develops an IDS signature, and Nation C tests the patch in their lab environment. The coalition collectively benefits by providing better overall service in a shorter timeframe with fewer national resources, leveraging the strengths and time zones of the various nations.

4.2 Deployed Theatre Operations – Shared Intrusion Detection System (IDS) Data

In this scenario coalition forces are deployed in a theatre operation and the sharing of IDS information through a Coalition CND COP allows the discovery of a new stealthy attack. Military operations are heavily dependent on the networks for: exchanging C2 information between national theatre C2 systems using the Joint Command, Control, and Consultation Information Exchange Data Model (JC3IEDM) standard; Voice over IP

(VoIP) for orders planning, logistics, and other non-combat communication; and collaborative applications such as chat.

In this scenario, it is assumed that both national and coalition network assets are at the Secret level. There are no direct external coalition network connections; however, each nation retains a Secret link back to their national strategic Secret network. There are complex guard/gateway functions joining the various coalition member theatre networks to ensure caveat separation. Nations provide in-theatre security personnel (that is, security is managed locally and not from each coalition member's strategic home network).

Flow of Events

1. Through human error, Nation A personnel installs a self-propagating piece of malicious code on a workstation within their network. The code is slow-spreading and targeted to propagate like VoIP data in order to move through coalition gateways in a stealthy manner. It is made to look, from a user perspective, like someone is calling and hanging up.

2. National IDSes raise suspicious traffic alarms and this information is automatically shared through and fused by the Coalition CND COP. IDS events are correlated and based on the aggregate information it appears as though malicious code is propagating through the coalition network. Through mathematical analysis of the fused Coalition CND COP data it is concluded that the call/hang-up pattern has a strong periodicity, implying an automated attack.

3. Security and network analysts collaborate and examine the network topologies through their CND COPs and the Coalition CND COP to determine which VoIP phones are infected and how to mitigate the malware propagation with the least operational impact. One of the nations has not yet been infected.

4. The coalition commander is notified through the Coalition CND COP that there is no immediate impact to his operations. However, the recommended COA is isolation of the infected 30% of total VoIP hosts (this assumes there is a low-level safeguard like a host intrusion prevention system or a VoIP management platform to blacklist individual phones) in addition to isolation between nations until the malware propagation can be stopped. The coalition commander approves the recommended COA.

5. The CND analysts isolate the infected VoIP phones and national networks.

6. In the meantime, the analysts collaborate using the fused information in the Coalition CND COP and national logs to trace the propagation of the attack, thus finding the original source. Also, they isolate a copy of the malicious object code. The code is reverse engineered to determine its trigger mechanism and impact. The trigger mechanism is a specific future date and the information is shared through the Coalition CND COP.

7. Intelligence analysts are aware of this date based on other sources and conclude that this date will likely coincide with a physical attack against coalition forces. The commander is made aware of this through the Coalition CND COP.

8. Nation A's intelligence team determines that the malware was introduced on a Universal Serial Bus (USB) key through social engineering.

9. The nations configure virus scans on each host that force removable media device scanning prior to use and the national networks are reconnected.

10. The infected phones are refurbished by reinstating the last good software load with a patch for the vulnerabilities exploited by the malware.

Discussion

IDS information is automatically shared with all coalition members so the extent of the attack can be understood sooner. One nation was protected due to the speed of detection and the rate of reaction, which is far less likely without automation. Sharing IDS information gives a better understanding of adversary capability since the trojan behaviour is observed across the coalition network, rather than on a single network, and the periodic behaviour can only be observed at the coalition level. In this scenario, CND analysts are deployed in theatre. Collaboration between analysts for problem solving across the coalition would allow for a sharing of resources in this respect.

The COA was coordinated throughout the coalition by looking at the overall situation and engaging the coalition commander. This resulted in an informed COA where the risks are understood, as opposed to an immediate reaction by nations without an understanding of the impact on operations. In addition, correlation of the trigger mechanism and intelligence information through the Coalition CND COP made the coalition commander aware that activity on the networks may be related to possible physical attacks.

4.3 Deployed Theatre Operations – Virtual Machine (VM) Migration

In this scenario a physical attack on a deployed coalition member's network assets results in a reconfiguration of C4ISR applications across the coalition. The Coalition CND COP allows the sharing of large volumes of complex information and provides awareness of available resources among coalition members to support COA decision making. It is assumed there is full knowledge of asset criticality both to the nations and to the coalition at all times.

This scenario assumes that a coalition is making extensive use of VMs in theatre to achieve greater survivability and availability of C4ISR applications, such as supply, fire control, targeting, VoIP phone, web sites, databases, collaborative tools, email servers, etc. Coalition personnel access the C4ISR applications using local workstations over the coalition network. The applications run as VMs, hosted on physical servers that reside in tactical vehicles. Both redundant physical servers and server vehicles are provisioned and each nation manages their VMs and assets using a VM management system. Coalition members have compatible VM infrastructures in order to coordinate the migrating of

C4ISR applications between coalition members. In this environment it is foreseeable that members may provide redundant physical server capacity to other coalition members in the interest of keeping critical C4ISR applications running. This scenario explores such a situation.

Flow of Events

1. A mortar attack on the Nation A base destroys one of several vehicles containing C4ISR application servers.

2. Nation A's VM management system detects a loss of multiple C4ISR VMs, which is reported to the CND COP. The CND COP automatically correlates the loss of these VMs as being on the physical servers within a single vehicle. This event is automatically reported to coalition members using the Coalition CND COP so that all nations are aware of the loss of the C4ISR applications.

3. Nation A, assisted by its VM management system, determines a new configuration of VMs on the remaining C4ISR application servers to minimize the impact on operations. However, Nation A no longer has enough server capacity to run all the VMs and the coalition commander decides to stop low-priority VMs and to restart lost high-priority VMs from a recent (30 minute old) backup.

4. Nation A's CND COP automatically reports the new VM configuration and the time to repair to coalition members through the Coalition CND COP.

5. Coalition operations result in some of the stopped low-priority VMs becoming mission critical. Since Nation A no longer has sufficient physical server capacity to run them, they request VM server resources from coalition members through the Coalition CND COP.

6. The Coalition CND COP allows analysts among the coalition members to negotiate the VM resource requests from Nation A. Nations B and C have spare physical server capacity and agree to house the coalition VMs. The firewalls and VPNs are configured to backhaul the remote VM to Nation A's network.

7. Nations B and C restart the VMs with their VPN network connections backhauled to Nation A's network and full operations capability is restored.

Discussion

The volume and complexity of the sensor and configuration information that is shared necessitate the use of an automated Coalition CND COP in this scenario. The automated detection of C4ISR applications going offline allows all coalition members depending on those applications to get near real-time notification of their unavailability. Nation A's CND COP had the ability to determine that all of the C4ISR applications that went offline were housed in a single vehicle and to start reacting, including notifying coalition members. As part of the COA, the Coalition CND COP must exchange complex IT configuration information including VPN specifications, firewall rule adjustments, etc.

Additionally, the VM backups for the C4ISR applications represent a very large volume of information to move.

This scenario demonstrates the efficient use of coalition resources. The physical attack on one member reduces their IT capability below the threshold required to sustain coalition operations. However, knowledge of the coalition needs allows for the correct prioritization of VMs, and the efficient sharing of available IT server capacity among coalition members means the coalition operations are minimally impacted. One could extend this scenario to allow for more optimal deployment of IT resources among coalition members. For example, rather than each nation having twice their required IT server capacity for availability under their control, they might be able to deploy with 1.5 times the capacity and then manage the spare capacity across the entire coalition.

5. Benefits

In this section, several overarching benefits of a Coalition CND COP are presented. The next section outlines research required to achieve a Coalition CND COP capability, during which further benefits will become apparent. As demonstrated by the scenarios, obvious benefits of an automated Coalition CND COP include:

• Clearer SA. Collective, shared CND information can present a clearer SA picture that is not evident to individual coalition members due to improved observation and orientation phases of the OODA loop. The automatic exchange of consistent IA information and the ability to fuse the information from coalition partners provides better insight into the defensive posture of both national networks and the coalition as a whole. Additionally, knowledge of adversary computer network attacks on coalition members can be a forewarning to other coalition members of possible attacks.

• More efficient use of resources. A C2 COP attempts to provide a more efficient use of coalition battle resources to the force commander by providing a clearer operating picture. Likewise, a Coalition CND COP provides IA efficiencies that can result in resource efficiencies with respect to not only networks but also staffing and processes. Automating the sharing process allows for the removal of slow, centralized human-in-the-loop release authorities. Information ownership and release labelling means that the labels follow the information as it transits through the Coalition CND COP. This meta-data would provide the means to allow national guards to decide what information can flow to which coalition members in an automated fashion without human intervention. This would reduce the need for existing centralized personnel that authorize information release.[2] Furthermore, the automated exchange of Coalition CND COP information allows for the sharing of IA workloads among coalition members (provided the trust

[2] There are many instances when automatic decisions can be made based on a set of rules, but there are more complex situations which require human decision making. Ultimately we promote moving towards a more automated world because there are many complicating factors with humans in the loop, but we recognize that there are situations and circumstances that require and benefit from human involvement.

relationship exists). CND analyst functions could be distributed throughout the coalition allowing similar work to be done with fewer analysts or a heightened capability with the current number of analysts.

• More effective CND action. A Coalition CND COP with an automated information exchange supports rapid time scale, high volume, complex data exchanges without errors and omissions due to human processing and enhances coordinated CND activity across coalition boundaries. Being able to coordinate complex network activities enables a commander to take a more effective CND COA and allows coalition members to coordinate network activities in real-time. The precise coordination of events for computer network operations across the coalition network would be difficult without some form of automated information exchange.

6. Areas Requiring Research

This section is intended to identify research areas with respect to coalition CND information sharing in order to further refine concepts for practical, shared solutions. Benefits of the successful implementation of the research, while not necessarily highlighted in each case, should be evident. Caveat separation, secure labelling, and secure guard functionality are examples of areas requiring research to allow coalition members to securely exchange information of any type (applicable to all COPs). Other efforts, such as the Coalition Secure Management and Operations System (COSMOS) [21] and SAMSON, are looking into technologies and architectures that deal with these issues and are not addressed here. The research areas we address are categorized and introduced in order of priority.

6.1. Information Requirements for Coalition CND SA

Specifying the Information to be Shared. The information and level of detail of information that needs to be shared to do effective CND involving coalition members is not readily apparent. Specifying the information required is a step towards providing coalition CND SA. As illustrated by the scenarios, the degree of information sharing can vary greatly and the information sharing requirements may differ by situation. Relevant IA information may include available IT services, IT infrastructure, vulnerabilities, safeguards, exploits, threats, alarms, and incidents.

Integrating Network Management and Network Security. Network management and security have developed as distinct and separate areas of expertise; however, they are so closely intertwined that it is increasingly difficult to do one without the other. JNDMS demonstrates the successful integration of network defence and management into one system with the intention of being used by both network security analysts and network operations management staff. An underlying assumption of the Coalition CND COP is that nations adopt a similar view of CND SA in developing their CND COPs. This requires the research and development of algorithms to extract meaningful information from network management and security tools.

CND Information Fusion. Information fusion helps in dealing with the large volume of CND data, reputed for redundancy/overlap, false positives, and cross-correlation. Fusion should allow for the drastic reduction in these, resulting in a reduced data set for further fusion and smaller volumes of exchanges between partners. Within a CND COP, information fusion must occur to perform defensive posture assessments, recognize incidents, and perform severity assessments. This involves functions such as analysing information from datasets, identifying incidents, filtering information, correlating information, assessing incident damage, assessing the risk of incidents, and assessing incident severity. This becomes even more challenging across national boundaries where data is potentially sanitized and/or processed beforehand.

6.2. CND Information Sharing Issues

CND Information Classification. CND information must be properly classified and dealt with so that it can be processed in an automated fashion. The mapping of types and the level of detail of CND information to classification levels needs to be specified and the impact of the aggregation of information on classification must be understood; this is likely best determined by CND specialists. Given the automatic sharing of information among coalition members, there must be a method for tracking the ownership of information and allowing the information to be released only with the owner's approval. This likely requires a system that can securely label information in terms of ownership and its release outside the originating nation and verify that coalition partners are not trying to release information without the consent of the originating nation. Furthermore, information to be shared within a coalition must be classified by the originator so that coalition partners who need it, get it. "Write-for-release" is a U.S. intelligence initiative that encourages information sharing with foreign partners by writing intelligence information so that it can be released by foreign disclosure officers [29]. This type of initiative needs to be encouraged in the CND information sharing community.

Influencing CND Information Sharing Policies. A better understanding of what needs to be shared would give a clearer understanding of the constraints imposed by current CND information sharing and classification policies, along with the potential to positively influence them. National policies on how to classify information exist, however they are static and don't necessarily to apply to individual situations. Factors such as time criticality, trust, and operational necessity could impact the importance of CND information sharing, and the ability to dynamically re-adjust to the threat by changing policy, for example, could provide major benefits.

Sanitizing CND Information. Given the assumption that the level of trust will always be an issue for sharing in a coalition environment, methods of optimizing CND information sharing are required. Sanitizing data, such as by anonymizing identifying information, can make users more willing to share their information. For example, the SANS Internet Storm Center allows participants to submit firewall logs anonymously. They claim that it was only in the regional and global aggregate views of shared intrusion detection logs that the Lion worm attack was obvious [4]. Methods of sanitization across coalition boundaries and the effects of fusing sanitized or filtered information need to be examined.

6.3. Implementation of a Coalition CND COP

Development of a CND Data Model. Coalition IA information exchange systems need to be interoperable. One way to achieve the automated exchange of information is by using a data model that describes the semantics and syntax of the CND information to be exchanged as well as standards for the information labels. Existing CND COP systems may adopt this CND data model when exchanging information with coalition partners, which will require either internal changes to use the model, or building a translation function between internal models and the new exchange model. The data model must ensure that adequate network contextual information is exchanged so that the information passed has meaning within the coalition mission. For example, a Nation A server being down might be the semantics of the information passed to Nation B; however, knowing that B's mission depends on the A server information provides the appropriate network context to make the information exchanged meaningful.

Several network security data schema have been developed, such as M2D2 [25], Common Vulnerability Scoring System [26], and the Intrusion Detection Message Exchange Format [7], but none that completely supports the information requirements for CND SA as described in Beaudoin et al. [1], including IT services (and their importance to operations), IT infrastructure, vulnerabilities and safeguards, exploits, threats, alarms, and events. A data model to support these broad requirements for CND SA is a very important and complex component of a Coalition CND COP.

Figure 2 illustrates a simplified data model for the main elements of Defence Research and Development Canada's Impact Assessment Tool, a CND SA tool that has been used by operators at the CF Network Operations Centre to assist in understanding the impact of network events on operations. This indicates, at a very basic level, the type of model needed and relationships between the elements.

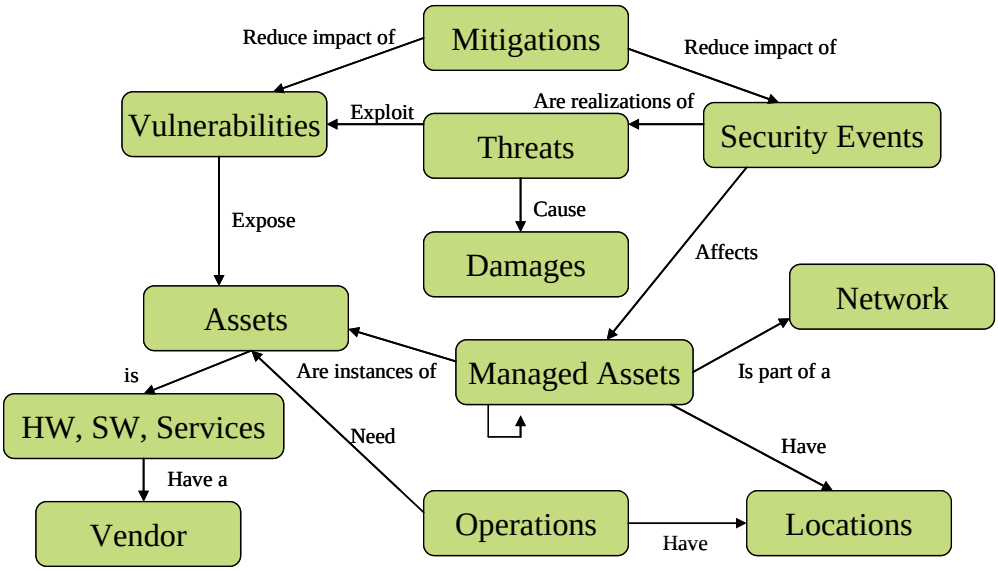

Figure 3. Simplified Data Model

COSMOS had identified IA as a community of interest that could benefit from an extension of MIP's JC3IEDM [27]. MIP's aim is to "achieve international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to the lowest appropriate level in order to support multinational, combined and joint operations and the advancement of digitisation in the international arena, including NATO" [28]. MIP is attempting to achieve information flow in a coalition C2IS environment through the definition of a common exchange data model and exchange mechanism. A Coalition CND COP requires the use of an automated information exchange mechanism similar to, or a subset of, MIP.

CND Information Visualization. The visual representation of CND information is a key component of a Coalition CND COP. NATO's Research and Technology Organization Research Task Group IST-059/RTG-025, Visualising Network Information, "interprets visualization as a human activity supported by technology. It is a means by which humans make sense of complex data." [22]. CND information visualization involves similar issues, requiring a display that is user friendly and allows the user to do a visual analysis for SA. The information required for CND SA is user-dependent and a function of the user's role, which implies that the information display will need to be versatile and allow for layers of granularity. JNDMS supports user-defined views and queries and allows users to visually correlate complex data from different domains: military operations, IT infrastructure and services, vulnerabilities and exploits, safeguards, and security events. Work in the commercial sector for network management can be drawn upon for CND visualization; examples of popular commercial network management products with visualization include netViz [23] and IBM Tivoli [24].

Integrating CND COPs into C2 Systems. Due to the reliance of operations on networks and to achieve increased CND SA among general military staff, national and coalition CND COP systems should be integrated with their corresponding C2 COP systems. This integration may take the form of a single integrated COP system, or separate systems that exchange the required information.

7. Conclusion

In this paper we have presented the vision for a Coalition CND COP, which is a means of providing CND SA in coalition operations. This system automates the exchange of both network management and security information and is part of the overall C2 system. While CND information exchange occurs on a basic level between some nations, a Coalition CND COP does not currently exist; however, as demonstrated in several of the scenarios, significant benefits can be gained through an automated Coalition CND COP with even a small degree of information sharing. A Coalition CND COP may become an operational necessity when coalition cyber operations become more prevalent. The vision and numerous research gaps detailed in this paper can function as a starting point for developing such a capability.

Glossary

C2	Command and Control
C2IS	Command and Control Information System
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIA	Coalition Information Assurance
CND	Computer Network Defence
CF	Canadian Forces
COA	Course of Action
COP	Common Operating Picture
COSMOS	Coalition Secure Management and Operations System
IA	Information Assurance
IDS	Intrusion Detection System
IST	Information Systems Technology
IT	Information Technology
JC3IEDM	Joint Command, Control, and Consultation Information Exchange Data Model
JNDMS	Joint Network Defence and Management System
MIP	Multilateral Interoperability Programme
NATO	North Atlantic Treaty Organisation
NVAT	National Vulnerability Assessment Team
OODA	Observe, Orient, Decide, Act
RTO	Research and Technology Organization
SA	Situational Awareness
SAMSON	Secure Access Management for Secret Operational Networks
U.S.	United States
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network

References

1. L. Beaudoin, M. Froh, M. Gregoire, J. Lefebvre, Computer Network Defence Situational Awareness Information Requirements, Paper presented at Military Communications Conference (MILCOM) 2006, October 23-25, 2006 in Washington, D.C.

2. J. Lefebvre, M. Gregoire, L. Beaudoin, J. Treurniet, Joint Network Defence and Management System – Concept Document, DRDC Technical Memorandum, DRDC Ottawa TM 2003-230, December 2003, limited release.

3. International Policy at a Crossroads, Canada's International Policy Statement, retrieved December 2007 from http://geo.international.gc.ca/cip-pic/ips/ips-overview3-en.asp

4. About the Internet Storm Center, The SANS™ Institute, retrieved December 2007 from http://isc.sans.org/about.html

5. M. Jahnke, M. Bussmann, S. Henkel, J. Tolle, Components for Cooperative Intrusion Detection in Dynamic Coalition Environments, Paper presented at RTO IST Symposium on Adaptive Defence in Unclassified Networks, RTO-MP-IST-041, April 19-20, 2004 in Toulouse, France.

6. J. Tolle, M. Jahnke, N. gentschen Felde, P. Martini, Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System, Paper presented at Military Communications Conference (MILCOM) 2006, October 23-25, 2006 in Washington, D.C.

7. H. Debar, D. Curry, B. Feinstein, The Intrusion Detection Message Exchange Format (IDMEF), RFC 4765, March 2007, retrieved December 2007 from http://www.ietf.org/rfc/rfc4765.txt

8. B. Feinstein, G. Matthews, The Intrusion Detection Exchange Protocol (IDXP), RFC 4767, March 2007, retrieved December 2007 from http://www.ietf.org/rfc/rfc4767.txt

9. USJFCOM, DISA, Coalition - Information Assurance Common Operational Picture - Advanced Concept Technology Demonstration (C-IA COP ACTD) FY03-07 - CONOPS, dated 05 May 2004.

10. J. Rogin, Cross-Domain Solutions Needed in Iraq, FCW.com Story, January 29, 2007, retrieved December 2007 from http://www.fcw.com/online/news/97504-1.html

11. D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, Inside the Slammer Worm, IEEE Security and Privacy Magazine, July/August 2003, pp 33-39

12. Intellitactics, Inc., retrieved December 2007 from http://www.intellitactics.com/int/

13. ArcSight, retrieved December 2007 from http://www.arcsight.com/

14. netForensics, retrieved December 2007 from http://www.netforensics.com/

15. MIP Tactical C2IS Interoperability Requirement (MTIR) Version 3.6, Multilateral Interoperability Programme, February 16, 2007, retrieved December 2007 from http://www.mip-site.org/publicsite/04-Baseline_3.0/MTIR-MIP_Tactical_C2IS_Interoperability_Requirements/MTIR%203.6%20Main%20(Ch%201,%20Ch%202,%20Ch%203)_FinalChecked.pdf

16. NATO Working Group 1 Report, Towards a Structured Approach for the Development of a Purpose Driven COP System, part of NATO Workshop Report RTO-MP-IST-043,Visualisation and the Common Operating Picture, December 2005

17. G.M. Perez, A.F.G. Skarmeta, S. Zeber, J. Spagnolo, T. Symchych, Dynamic Policy-Based Network Management for a Secure Coalition Environment, In *IEEE Communications Magazine*, November 2006, pp 58-64

18. S. Zeber, B. Carruthers, A. Magar, E. Bacic., SAMSON TD Concept of System Operations, DRDC Ottawa TM 2006-119, June 2006

19. R. Meushaw, D. Simard, NetTop – Commercial Technology in High Assurance Applications, National Security Agency Tech Trend Notes, Vol. 9, Ed. 4, Fall 2000

20. R.V. Meushaw, M.S. Schneider, D.N. Simard, G.M. Wagner, Device for and method of secure computing using virtual machines, United States Patent No. US 6,922,774 B2, 26 July 2005

21. Coalition Secure Management and Operations System (COSMOS) Advanced Concept Technology Demonstration (ACTD) Concept of Operations (CONOPS), Publication 3001, Version 1.0, December 10, 2005, For Official Use Only

22. Visualising Network Information, NATO Information Systems Technology IST-059/RTG-025, retrieved December 2007 from http://www.vistg.net/

23. netViz, retrieved December 2007 from http://www.netviz.com/

24. IBM Tivoli, retrieved December 2007 from http://www-306.ibm.com/software/tivoli/

25. B. Morin, L. Mé, H. Debar, M. Ducassé. 2002. M2D2: A Formal Data Model for IDS Alert Correlation. In *Lecture Notes in Computer Science*. 2516: 115-137

26. Common Vulnerability Scoring System (CVSS), retrieved December 2007 from http://www.first.org/cvss/cvss-guide.html

27. M. Laurine, Col. K. B. Jordan, Coalition Secure Management and Operations System (COSMOS), A Role-Based Access and Privilege Model for Coalition WAN Operations, Powerpoint Presentation, DISA, Brief for NCES/IPT 15 September 2004

28. Multilateral Interoperability Programme, retrieved December 2007 from http://www.mip-site.org/011_Public_Home_Concept.htm

29. Akers, Tyler. 2007. Taking Joint Intelligence Operations to the Next Level. In *JFQ* 47: 69-71