A Decision Timeline Approach to Assessing Air and Maritime Capabilities

Etienne Vincent

Neil Carson

NORAD Operational Research Team
Centre for Operational Research and Analysis
Defence Research and Development Canada
Peterson Air Force Base, Colorado Springs, Colorado, United States
e-mail: Etienne.Vincent@Forces.gc.ca

Dr. Etienne Vincent and Mr. Neil Carson are Defence Scientists within the North American Air Defence Command (NORAD) Operational Research Team of Defence Research and Development Canada's Centre for Operational Research and Analysis. This team provides Decision Support advice to the NORAD Deputy Commander, having recently focused in the areas of capability and vulnerability assessments through the development and application of threat and force response models. Etienne graduated from the University of Ottawa with a Ph.D. in Computer Science, and Neil from the University of Victoria with a Master of Applied Science in Electrical Engineering.

INTRODUCTION

The North American Air Defence Command (NORAD) is a bi-national (Canada-U.S.) military command tasked with aerospace warning, aerospace control, and maritime warning of threats to North America. These missions involve detecting and investigating all potential air threats and warning of all potential maritime threats approaching Canada and the United States. The air and maritime threats to North America potentially range from state adversaries, to terrorism, to illicit trade.

NORAD Operational Analysts have long studied national response capabilities and vulnerabilities against potential air and maritime threats. A decision timeline approach has evolved to address these assessments. The decision timeline approach has been applied to NORAD's capability to warn and respond against various threats, including small aircraft involved in illicit trade, vessels involved in human trafficking or the importation of weapons of mass destruction, undeclared penetrators of air defence identification zones, airborne terrorists, and cruise missiles. These assessments have improved understanding of NORAD's battlespace and informed changes to its force posture, as it adapts to new and evolving threats.

This paper presents the decision timeline framework, highlighting its advantages of revealing all defensive gaps that could be exploited by the considered threats, and of providing a visualization of these gaps that often suggests solutions. The approach will then be illustrated with representative examples from applications to the defence of North America.

ASSESSING DEFENSIVE CAPABILITIES

Forces that are assigned defensive responsibilities, such as NORAD, should continuously assess the vulnerability of their defences. Vulnerability may change as new threats appear, existing threats develop new capabilities, or the defensive forces' own capabilities are enhanced or degraded. Furthermore, planning requires assessments of the impact of considered force posture modifications or equipment acquisitions on defensive capabilities.

Typically, a standard to be met guides the assessment. As an example, when assessing surveillance capabilities over the waters surrounding an island that is to be defended, a surveillance requirement can be defined. This requirement could state that all threats of a given type are to be detected outside of a fixed specified range from shore. That range from shore would be set as sufficient to allow the defending forces to respond and counter threats. If the threats considered in the assessment were smuggling craft, the surveillance requirement could be set to a distance sufficient to provide law enforcement authorities enough time to intercept detected smugglers before they land and unload their illicit cargo.

Figure 1 illustrates a notional fixed surveillance requirement (shown in light blue) around an island. Approaching threats would have to be detected before penetrating that zone.

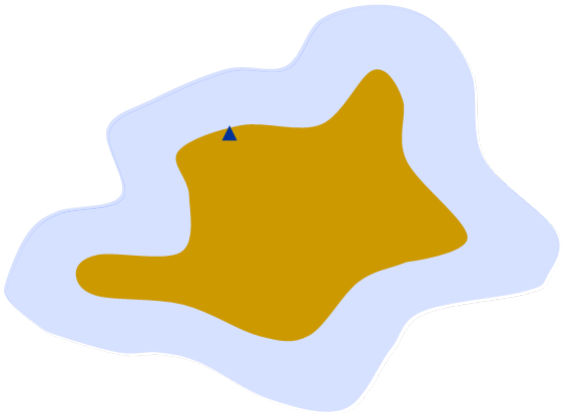

Figure 1. Notional surveillance requirement for the waters around an island

A surveillance requirement can then be compared to actual or planned defensive capabilities to see if it can be met. The requirement shown in Figure 1 could be compared to the sensor coverage provided by existing sensors. Requirements for other aspects of the defences (e.g. responding interceptors, communications, etc.) can similarly be assessed.

The potential weakness of this approach is that the vulnerability assessment it produces is only as good as the established requirement. An invalid requirement will yield an incorrect assessment. For example, in Figure 1, if the blue triangle represents the location of the alert site where responding forces are based (e.g. a helicopter that will intercept the smuggling craft), then the defensive force's response will be quicker near that site. Thus, close to the site, a response can be initiated when the threat is closer to shore, and consequently, surveillance near the alert site needs not extend as far offshore. The surveillance requirement shown in Figure 1 would thus have exceeded the true requirement near the alert site, and could result in unnecessary investment in additional sensors.

INVESTIGATING MISSION REQUIREMENTS

The example of the previous section highlights the importance of working with the correct requirements. It is often beneficial to review mission requirements before engaging in a capability assessment. At NORAD, this typically means that surveillance and response must be considered together. The typical NORAD intervention is a sequence of events that begins with an initial warning of an approaching threat and ends with its intercept and neutralization. Any requirement to detect all threat beyond a fixed distance or for responders to reach all defended points within a given time delay is necessarily artificial. What is important is for the initial warning to be generated early enough to enable a response that results in a timely intercept. Defining a requirement that encompasses both surveillance and response will result in fewer false or missed capability gaps in the resulting assessment.

Figure 2 illustrates the process whereby defensive capability gaps should be identified and closed. Gaps are identified through the juxtaposition of capabilities and requirements, with the assessment of requirements tied to mission success criteria and deserving full consideration. Once valid gaps are identified, they are to be closed at a minimal cost, which may be achieved through the re-deployments of existing systems or the revision techniques, tactics and procedures. The capability enhancements may be targeted at improving capabilities or at reducing mission requirements (e.g. at improving surveillance or at reducing the need for surveillance). Expensive acquisitions or investments in research and development only become necessary when gaps persist.

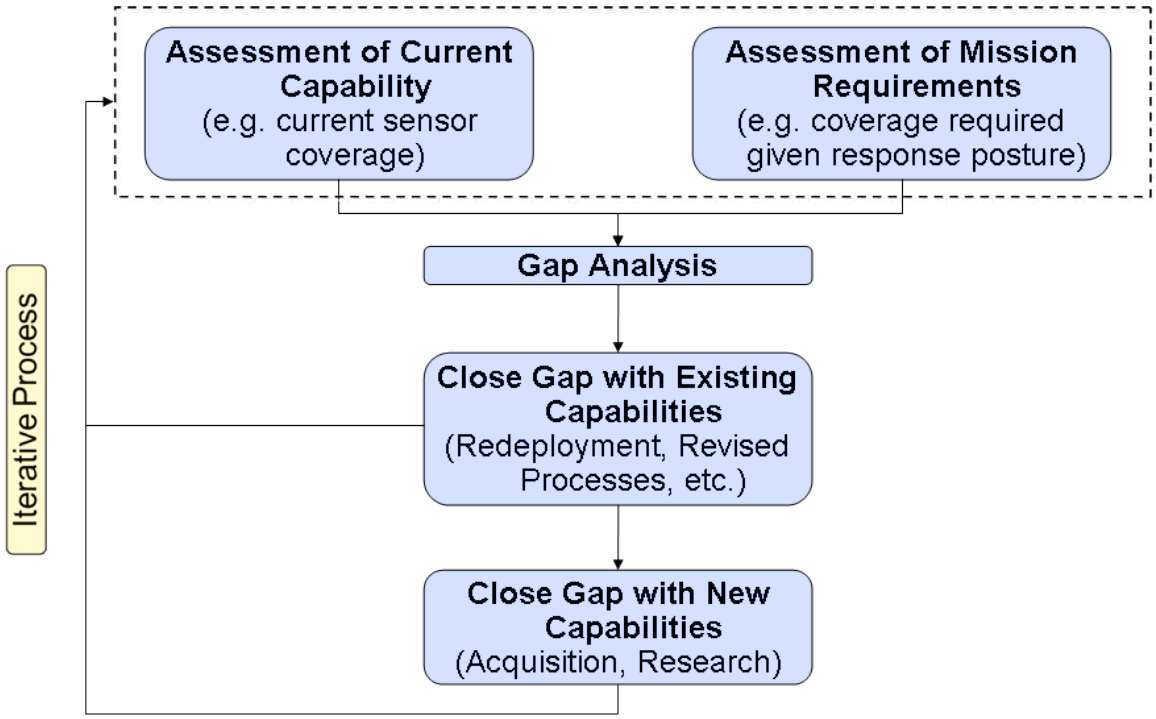

Figure 2. Capability gap assessment process

A direct method for considering capabilities and mission requirements together in a gap analysis is to perform simulation. This entails modelling defences and representative threats, and executing simulation runs of representative scenarios to see which threats can or cannot be neutralized. For the previous example of surveillance of an island, this would involve modelling sensor coverage as well as responder capabilities. Modelled threats approaching at a given speed along a given axis can then test these defences. A response is initiated as a threat penetrates sensor coverage. If the sequence of events that follows leads to intercept of the threat before it reaches shore, the threat is neutralized. Otherwise, a gap is identified. Figure 3 illustrates such a gap analysis performed through simulation. Sensor coverage is shown as pink circles, the responding forces' alert site are shown as a blue triangle, and threat axes are shown as dashed lines. The green dashed lines represent mitigated threats, while the red ones represent vulnerabilities. To close the identified defensive gaps, modifications to the defences can be modelled, and additional runs of the simulation performed to see which of the introduced modifications neutralize the threats. The modifications to the defences could include new or improved sensors, more alert sites, faster response platforms, or changes to the processes that trigger responses, which could shorten delays.

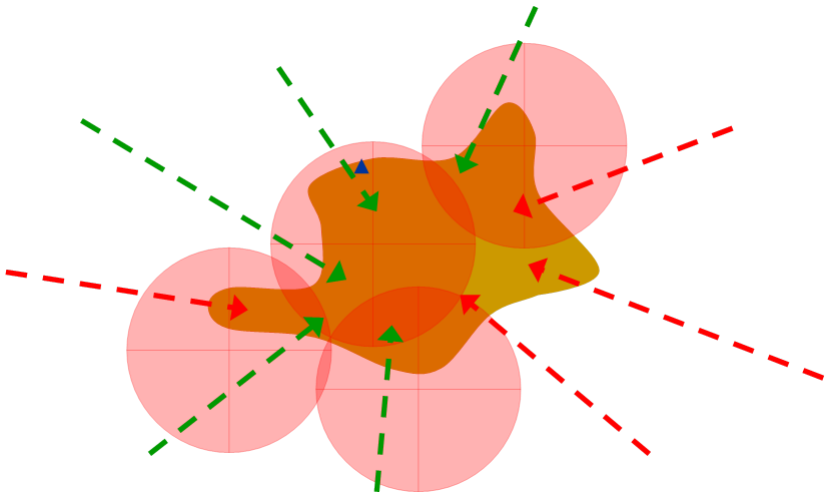

Figure 3. Notional example of a simulation study to address capability gaps

In Figure 3, five of the nine threats considered are shown as having been neutralized. It is important to understand that this does not mean that the defences are effective $5/9^{th}$ = 56% of the time. In fact, the threats drawn in red will achieve their objective 100% of the time. Since the choice of a means of attack lies with the opponent, any gap known to that opponent can be exploited, whereas approaches known to be defended are unlikely to be tested.

The simulation approach to assessing capabilities illustrated in Figure 3 suffers from some weaknesses. The principal one is that it is somewhat anecdotal, in the sense that it only highlights the gaps that have been tested. There is no way of knowing if an additional threat approach would reveal an additional gap, other than to use it in an additional run. A related weakness is that the simulation does not immediately provide explanations for the gaps and provides little information that may help close those gaps. Investigation of the gaps and the development of solutions for closing them require separate analysis. The following section describes an alternative approach to simulation and highlights some of its advantages.

THE DECISION TIMELINE APPROACH

The decision timeline approach addresses the capability assessment problem by considering the scenario timeline in reverse-chronological order to establish requirements. Figures 4-6 illustrate a simple example of a decision timeline analysis. In this example, threats attempt to reach an island's coast, while the defending forces attempts to counter those threats by reaching the targeted coastal points before the threats land.

First, in considering a single point to be defended, response time to that point is estimated. This requires a model of the responding platforms' capabilities, which can be fairly simple in many cases. For example, in the case where the responder is an aircraft and the distances involved are shorter than the aircraft's maximum range, the response time might be approximated as the sum of an alert time and flight time, the latter approximated as distance divided by speed.

With response time known, the position of an approaching threat at the time when response must be initiated can be determined. For example, Figure 4 illustrates the case where threats may be approaching a coastal point from any direction, at fixed speed. If the responding force is on alert at the base shown by a blue triangle, its response time will be a function of the distance from that base to the coastal point. If the defence is to be successful, the responding force must reach the coastal point no later than the threats. In the extreme case, the responding forces and threats arrive simultaneously. In that extreme case, response time and threat speed define the distance from the coastal point where threats would be located at the time when the response was initiated. That distance defines a circle around the coastal point called the *decision line*. It is the last threat location where a decision to launch a response can be made. In Figure 4, the decision line is shown as a dashed green circle. A response initiated before a threat crosses the decision line will succeed, whereas it may come too late if initiated when the threat is inside the decision line.

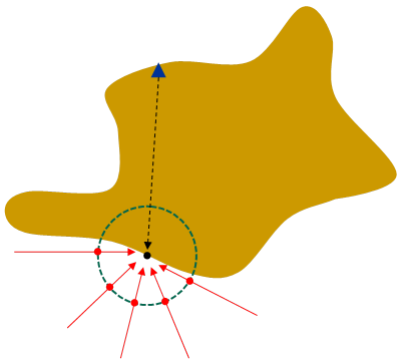

Figure 4. Decision line around a coastal point

Other lines can also be drawn to correspond to other milestones of the response timeline. For example a command and control delay may precede the initiation of a response. This delay from first detection of a threat to initiation of a response could be added to the response time to yield a *surveillance line* outside the decision line. Such a surveillance line around a coastal point is shown as a dashed blue circle in Figure 5.

The decision lines and surveillance lines around all defended points can then be merged to result in decision and surveillance lines for the entire theatre. In the considered example, the defences are to be for the entire coast of the island. Figure 5 shows the

decision and surveillance lines for the islands as respectively green and blue lines. These lines are closer to the coast nearer the alert site as response is quicker there.

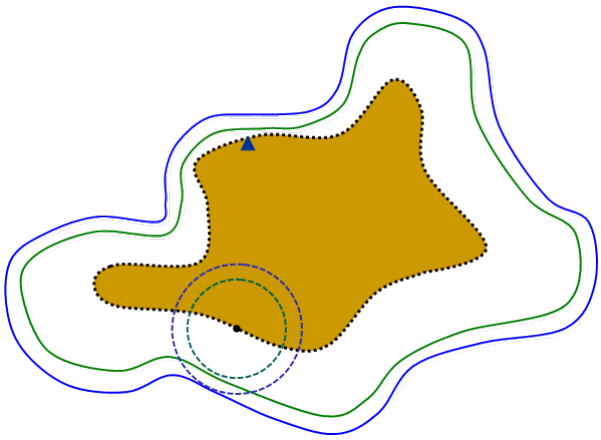

Figure 5. Decision and surveillance lines around the coast of an island

In Figure 5, the surveillance line represents the last point in the approach of a considered threat where detection may occur in time to trigger a response that will allow neutralization of the threat. The island will therefore be assessed as defended if detection outside the surveillance line is possible for any threat. That will be the case if surveillance extends to that line. To see if there are capability gaps in the island's defences, sensor coverage is overlaid on the surveillance line. In Figure 6, the pink circles again represent the coverage provided by four ground based sensors.

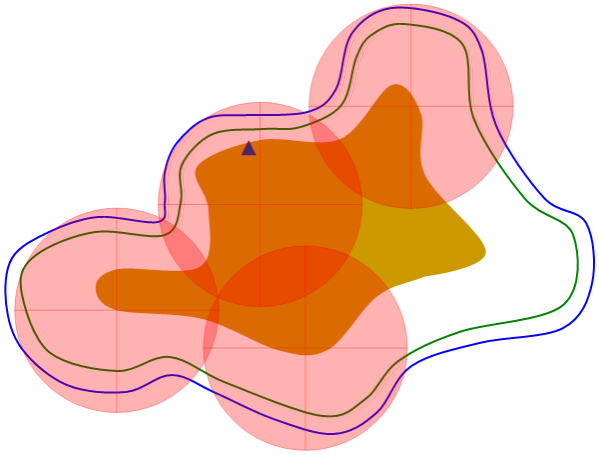

Figure 6. Capability gaps in the defences of an island

The capability analysis illustrated in Figures 4-6 clearly corresponds to a simple case, but application of the decision line approach to scenarios that rely on more complex defences or more detailed timelines is straightforward.

A first advantage of the decision timeline approach over simulation is that it reveals all defensive gaps with regards to the modelled threats, as it is not limited to a fixed number of considered threat approaches. The extent and the severity of the gaps are clearly illustrated by the juxtaposition of decision lines and sensor coverage. In Figure 6, for example, a gap that was missed in Figure 3 is now revealed in the lower-left. It is also seen that the previously identified gap at the leftmost tip of the island is not far from being closed. In fact, since the decision line lies within sensor coverage, a reduction in command and control delays may be sufficient to close the gap by moving the surveillance line toward the decision line. Another important advantage of the decision timeline approach is then that it provides an insightful visualization of capabilities and gaps, which in many cases suggests the appropriate solution to the gaps.

The remainder of this paper will briefly describe recent applications of the decision timeline approach in support of NORAD plans and operations.

APPLICATION TO ILLICIT TRADE INTERDICTION

NORAD assists law enforcement authorities in the detection and monitoring of aircraft suspected of involvement in illegal drug trafficking. To fulfill this mission, these aircraft must be detected in time to initiate a response that will result in their intercept. This is a straightforward application of the decision timeline approach. If an intercept is desired at the moment when a suspected trafficker enters sovereign airspace, response times to the border define a decision line away from that border. Surveillance coverage must extend at least up to that decision line.

APPLICATION TO MARITIME INFORMATION SHARING

In the maritime domain, threats travel more slowly, and distances can be great. Information on suspicious activity may be collected by many players, such as domestic and allied navies and law enforcement agencies, as well as commercial shippers. In addition to basic application of the decision timeline approach to establishing surveillance requirements, an application to information sharing requirements is possible. This involves establishing when the various players hoarding information on suspicious vessels must share it, if it is to enable an intercept before a vessel reaches its destination and achieves its aim. Targeted applications may range from interdiction of illicit trade including illegal immigration, to sea-based terrorism and attack by enemy navies.

To address maritime decision timelines, a toolset was developed at NORAD, which was described in a Phalanx article[1]. It provides a visualization of maritime warning requirements to show where decisions and information exchanges must occur. An important additional consideration for tools in the maritime domain versus the aerospace one is that land avoidance must be considered in the response time model. For this, the NORAD tool relies on an implementation of the Floyd-Marshall algorithm[2].

APPLICATION TO SOVEREIGNTY OPERATIONS

Canada and the United States enforce air defence identification zones (ADIZ) along their periphery. All aircraft approaching the North American landmass are required to provide a flight plan to air traffic control authorities. When an undeclared approach is detected, NORAD fighters may be sent to intercept the aircraft.

One type of incursion that regularly confronts Canadian and United States authorities is that of Russian Air Force long range bombers penetrating northern portions of the ADIZ. Response to these incursions requires enough warning to allow NORAD fighters to fly out and meet the intruders. The decision timeline approach is ideally suited to asses NORAD capabilities in this area.

If a specific intruder's flight path is considered, with a desired intercept point along it, an earlier decision point along that path can be computed. This point corresponds to the location of the intruder at the latest moment when an effective response can be initiated. The location of such points can then be compared to the capabilities of existing or anticipated sensors to see if they would provide the required warning.

One additional consideration, when it comes to northern sovereignty operations is that the intervening fighters may require air-to-air refuelling to reach remote intercept points. This makes the estimation of response time more complicated, requiring the development of an air-refuelled response time model.

APPLICATION TO AIRBORNE TERRORISM

NORAD's mission includes the defence of North America against airborne terrorist attack. One means whereby this could be achieved is through the intercept and possible engagement of airborne terrorist platforms by NORAD fighters. Again, capabilities in this area can be assessed using the decision timeline approach.

---

[1] N. Carson and J.D. Caron, "The Maritime Timeline Analysis and Requirements Toolset (M-TART)", *Phalanx*, Vol. 43, No. 4, Military Operational Research Society, December 2010.

[2] R. W. Floyd, "Algorithm 97: Shortest Path". *Communications of the ACM*, Vol. 5, No. 6, p. 345, June 1962.

In this case, the eventual engagement decision process is important to the decision timeline. Threats must be met away from their target to allow enough time to assess them and make a decision to engage. This defines an intercept line around a defended site. The decision line is then drawn away from that intercept line.

The sources of warning for such attacks can also be more varied than in the previously considered examples. Warning of the attacks of 11 September 2001 came from inside the hijacked aircraft (phone calls, loss of contact with air traffic controllers, deviation from declared flight routes, turning off of transponders). The decision timeline approach can yield decision lines around sites to be defended that show the warning required to intervene against such attacks. The amount and distribution of commercial flight traffic around the sites combined with decision lines then provide a measure of vulnerability to such attacks.

Another historical example of airborne terrorism is provided by the Tampa plane crash of 5 January 2002, when a Cessna 172 was stolen and crashed into the Bank of America Tower. In this case, warning came at the time of takeoff, as a result of the theft, prompting an interception by a United States Coast Guard helicopter that was nevertheless unable to prevent the crash. For such events, decision lines may provide information on the type of security measures that should be taken at airfields depending on whether they are located within selected decision lines or outside.

In some situations, temporary flight rules are applied to require the filing of flight plans for aircraft penetrating certain airspace. Such flight rules are, for example, employed around Washington, DC and frequently instituted above significant special events. These flight rules provide one means of identifying suspicious aircraft. To be effective, temporary flight rules must extend at least up to a decision line and have sensor coverage.

APPLICATION TO CRUISE MISSILE DEFENCE

A final application of the decision timeline approach at NORAD is in the assessment of its cruise missile defence capabilities. If missiles are to be intercepted by ground-based, seaborne or airborne platforms, decision lines again provide a means to assess response capabilities given available sensors.

The decision timeline approach can also be used to look at interventions against the launch platforms. Given that cruise missiles can travel over long distances, the defence of one site may require the capability to intervene along a very long perimeter, with surveillance capability required along a decision line that extends away from that perimeter.

CONCLUSION

This paper has described a decision timeline approach to assessing defensive capabilities. It has also briefly described some uses made of this approach by NORAD. The main benefits of the decision timeline approach over commonly used simulation studies are its ability to identify all defensive gaps, as it is not limited to a discrete set of considered runs, and the ease with which these gaps can be visualized, thereby suggesting solutions to closing them.