Radar Information Networks with Target Data Persistence for Intelligence-Led Border Enforcement

Tim J. Nohara, P.Eng, Ph.D, *Member IEEE*
Accipiter Radar Corporation, 40 Centre Drive, Orchard Park, NY, USA 14127
Tel: 716-508-4432 Fax: 888-393-6421 tnohara@accipiterradar.com

***Abstract*— Radar surveillance forms the foundation of many security strategies by providing enhanced threat awareness. For the security missions of the post 9/11 world, conventional radar lacks the connectivity, data persistence and user application infrastructure to be fully effective. With limited data persistence, there are only a few standard target data presentations or information products that serve to provide situational awareness to operators. If one retains for every target its attributes {latitude, longitude, altitude, speed, heading, size (RCS), versus time} 24/7/365 (i.e. data persistence is infinite), then an entire eco-system of information products containing high-value intelligence and situational awareness is possible with suitable application infrastructure. Furthermore, large and diverse numbers of remote users with their particular missions can have direct, secure access to authorized timely information; not just radar operators. Users involved in intelligence, interdiction, investigation, prosecution and resource management can all be readily served, providing force multipliers across the entire security enterprise without increasing the cost of the underlying radar surveillance network.**

Keywords-radar, surveillance; homeland; border; law enforcement; security; intelligence; force multiplier; threat; awareness; radar information network

I. INTRODUCTION

Surveillance forms the foundation of every security strategy by providing threat awareness. Radar is the gold standard for surveillance of potentially hostile, uncooperative targets. For the security missions of the post 9/11 world, however, where threats respect no boundaries of time or place, conventional radar lacks the connectivity, data persistence and user application infrastructure to be fully effective. Failures of radar because of these deficiencies are now shaping many homeland security procurements. Affordable radar networks have been developed, reported and field-tested that provide the connectivity needed for wide-area surveillance, by integrating target data from multiple radars [1]. This paper builds on that earlier work by presenting and discussing the issues and practical designs associated with data persistence and user application infrastructure.

Data persistence and user application infrastructure are related and interdependent. With limited data persistence, there are only a few standard target data presentations or information products that serve to provide situational awareness to operators. The design of these information products are typically tightly coupled to the radar processing system. On the other hand, if it is possible to retain for every target its attributes {latitude, longitude, altitude, speed, heading, size (RCS), versus time} 24/7/365 (i.e. target data persistence is infinite), then an entire eco-system of information products containing high-value intelligence and situational awareness is possible with suitable software application infrastructure. Furthermore, large numbers of remote and diverse users with their particular missions can have direct, secure access to authorized timely information; not just radar operators. Users involved in intelligence, interdiction, investigation, prosecution and resource management can all be readily served; and benefit from information products tailored to each without changing or increasing the cost of the underlying radar surveillance network.

The challenge is to build a practical target information system (TIS) with the desired data persistence and user application infrastructure. We present and discuss herein a TIS design which has been implemented, tested and deployed operationally. Technical issues addressed include target data asynchrony, data integrity, management and delivery, temporal and spatial target behavior exploitation, security, privacy, information sharing, and user-flexibility. A diverse set of information product examples taken from real-world radar networks are used to illustrate the concepts presented.

The potential to support intelligence-led law enforcement and serve as a real force multiplier across the entire security enterprise has never been so great. The TIS-based, user-centric (as opposed to radar-centric of the past) approach presented here is currently in operation, redefining radar for 21st century applications.

II. THE CASE FOR DATA PERSISTENCE AND USER APPLICATION INFRASTRUCTUURE

Simply put, it is not possible in border security applications, as it has been in military operations, to rely on a trained operator staring at a radar screen to detect all threats and report them in a timely manner to those who can mitigate them. The reasons for this short-coming are scope of operations, cost, threat behavior, and information overload.

In light of the above, target data persistence is needed to capture all target movements in the coverage volume so that they can be reviewed and analyzed on-the-fly as well as after the fact. In addition, a user application infrastructure is needed so that numerous, remote, non-radar-expert users can automatically receive user-specific, data-driven alerts as well as efficiently query the target data after the fact for any desired information.

This work has been supported indirectly by Defence Research Development Canada Centre for Security Sciences and the US Department of Homeland Security Science & Technology through operational deployments that have fostered direct contact between radar engineers and law enforcement personnel.

Presented at the
2012 IEEE INTERNATIONAL CONFERENCE ON TECHNOLOGIES FOR HOMELAND SECURITY
13-15 November 2012, Waltham, MA

A. *Data Persistence*

Many radar sensors are required to cover the thousands of miles of unmanned borders such as the Canada/US border for small targets including small vessels and low-flying aircraft. Governments can't afford to hire trained radar operators dedicated to each radar sensor as is done in the military. The end users of the target information are law enforcement personnel who have many duties that would be compromised if they had to be slaved to radar screens. They are also not trained radar specialists.

Watch-floor personnel in fusion centers are responsible for monitoring a variety of sensors and information sources and have to multiplex their time across various sensors and information sources. In addition, the watch-floor is often not fully staffed 24/7. As a result, a suspicious situation such as a rendezvous will be regularly missed if we were to only rely on real-time target tracks displayed on a screen (see Figure 1) with a dedicated operator. And suspicious activity that occurs after hours will routinely be missed without the aid of technology.

In military operations, the presence of an unknown target in the operating theatre is enough to make that target suspicious, as there are only friends and foes. This is not the case in the homeland. Threat behavior (i.e. suspicious activity) often takes a significant observation time interval to detect. Consider the following case which will be referred to as the *there-and-back border crossing* example. A vessel travels a couple of hours mid-day starting at a waterfront home on Lake Ontario in Canada near Toronto. The vessel crosses the Canada/US border, and stops and disappears off the radar at a US marina inside the border in western New York. A few minutes later, a vessel is tracked leaving the same marina. It crosses the same US/Canada border and continues over a couple of hours before it arrives at the same waterfront home in Canada. Only when it is determined that there is repeated movement between two cross-border locations does the activity become suspicious. But for this example, continuous observations for several hours would be required which is a cause for operator information overload, especially given these are just two of numerous vessels filling the display and vying for operator attention. The short time between the vessel arriving at the US marina and one leaving from it is suggestive that it might be the same vessel. Target analytics such as vessel dynamics and radar cross section profiles can assist in this determination, which would make the situation even more suspicious, likely triggering some level of intelligence gathering and investigation. If such behavior was timed to occur around shift-changes on the watch floor, it would be virtually impossible for watch-standers to *connect the dots on their own*. Without data persistence (and applications to characterize these long-duration trajectories and alert the operators), this pattern of behavior which took several hours to complete would go undetected.

In each of the above situations, data persistence provides the means of capturing target movements indefinitely, so that they may be recalled and reviewed as needed, after the fact, obviating the need for sole reliance on numerous, costly, highly-trained, dedicated operators.

B. *User Application Infrastructure*

Data persistence is not enough though. Tactical tools are needed to mine the data so that users can be alerted in real-time to threat situations and be provided with suspicious activity reporting. Pre-set alerts incorporating existing law enforcement and intelligence expertise enhance intelligence led enforcement capability. And strategic tools are needed to analyze the extensive target data sets built up over time to support a variety of analytical functions as described further below. The user application infrastructure provides interfaces to real-time and historical target data, supporting an arbitrary number of remote users running an arbitrary number of software applications to get the situational awareness they need.

A brief examination of the actors involved in the border-security enterprise and the information they require to carry out their respective missions demonstrate that one shoe does not fit all when it comes to exploiting target data. Rather, an eco-system of rich software applications is needed for maximum force multiplication. Building upon the aforementioned *there-and-back border crossing* example, we consider law-enforcement users with the following functions:

- interdiction;
- intelligence;
- investigation;
- prosecution; and
- management.

Interdiction. Interdiction requires tactical tools that provide immediate situational awareness along with near-term reach-back to targets of interest. Figure 1 is an example of such a tool that provides real-time locations for vessels on Lake Ontario. The Canada/US border is illustrated and vessels are shown crossing the border and heading towards Toronto. In this particular instance, a number of sail boats are involved in a 300 km race where one leg of the race begins near Youngstown, NY and ends near Toronto, ON.

A law-enforcement marine unit can be guided to intercept a vessel target of interest (TOI) using an on-board tactical display, or by being provided with target coordinates from a watch-stander running such a display on the watch-floor in a fusion center. When the marine unit conducts a spot check on the TOI, the vessel may be anchored several miles away from the border. In questioning the occupants, they may reveal that they are just hanging out in Canadian waters and have not crossed any borders. A target reach-back capability would inform the marine unit that the TOI had in fact crossed the border an hour earlier indicating that the occupants were lying. This would justify additional measures such as boarding and searching the vessel which may lead to an arrest and a seizure. Figure 2 illustrates this target reach-back for a target intercepted at 9:18 pm on 19 July 2010 during the sail-boat race. While intercepted several miles inside Canadian waters, law-enforcement personnel would know precisely when that vessel entered from the United States. They would also be alerted to the fact that this was a high-speed vessel not characteristic of the sail boats in the race. Target reach-back can also apply to multiple targets or a particular region for an arbitrary period of time.

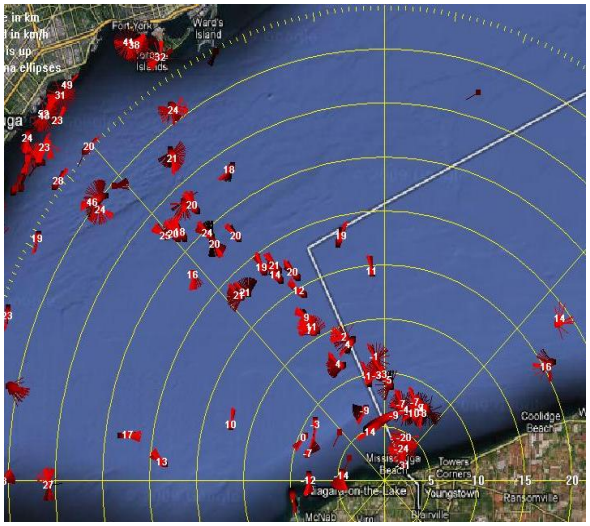

Figure 1. Real-time display of small vessels crossing border in afternoon of 19 July 2012. Radar located at Niagara on the Lake.

Figure 2. Target responsible for border crossing alert on 19 July 2010 between 9 to 10 pm local time (EDT) obtained through target reach-back.

The combination of real-time plus target reach-back can help uncover the suspicious behavior of the vessel in the *there-and-back border crossing* example. It can also help marine units quickly respond to a search and rescue call that would have otherwise kept them away from security operations all night. Consider a distress call received from a disoriented fisherman lost at 11:00 pm a couple of miles offshore on Lake Ontario in heavy fog. He advises he left a particular marina at 6:00 pm. With target reach-back for all targets leaving the marina around 6:00 pm combined with a real-time display, he can be found almost immediately. The target trajectory that ends at a current target location represents the lost fisherman. He can be safely guided back to shore over the phone, or quickly escorted by the marine unit.

Intelligence. Intelligence gathering requires analysis of current and historical target movements in search of suspicious activity including that based on existing information. Suspicious activity could be unusual discrete events or patterns of activity indicative of organized illicit operations. A variety of software tools support the intelligence analyst in mining the target data for such information. It is the intelligence analyst who would most likely discover the *there-and-back border crossing* which could then trigger an investigation.

A software application that continually generates, issues and stores border crossing alerts in the TIS can be quite useful. Figure 3 illustrates an example design of such alerts for the water border in the west end of Lake Ontario. Four polygonal zones are used (in this example) along with target heading information to discriminate and provide four different alerts: (1) West to East Canada to US, (2) East to West US to Canada, (3) North to South Canada to US, and (4) South to North US to Canada.

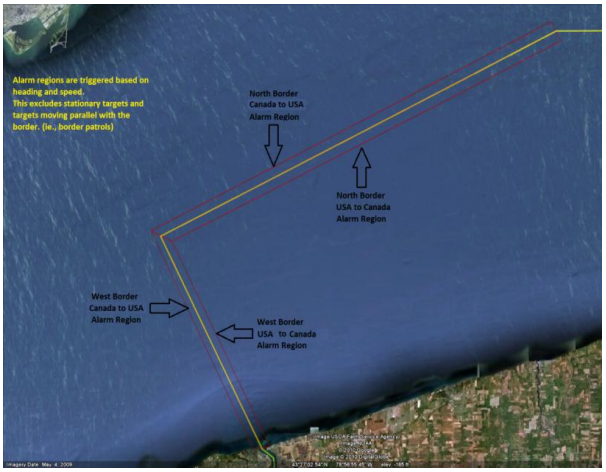

Figure 3. Four border crossing directions of interest.

The alerts can be acted on by the analyst in real-time, or they can be reviewed in batch, after the fact, such as the next day. The analyst triages the alerts. For each alert, the analyst quickly glances at a traffic history web page which organizes by year, month, day, and hour traffic summaries like that shown in Figure 4, giving the analyst a quick sense of vessel patterns and origins. Looking forward from the alert time, she can get a quick sense of where the vessel was heading to. Patterns of interest or ambiguities lead to further review. She can rapidly play back the actual target movements, pausing, single-stepping, and fast forwarding as needed for efficiency. A several hour sortie can be fully analyzed in a couple of minutes, including rendezvous detection. The trajectories from successive border crossings (such as the two crossings in the *there-and-back border crossing*) can be overlaid for significance.

A next day review of the previous night's border crossings using an approach similar to the above can yield timely and effective intelligence. As night-time activity is substantially reduced from the heavier daytime traffic levels, every night-time border crossing could be fully triaged cost-effectively.

Figure 4. Traffic summary from 1600 to 2100 on 19 July 2010.

In Figure 5, the border crossings by direction are illustrated for 19 July 2010, the same day of the boat race illustrated in Figures 1 and 4. The five-hour period used to generate Figure 4 is highlighted in Figure 5. The substantially lower border crossing levels during the night are clearly visible. On normal nights (i.e. without boat races), the number of crossings are even fewer. With a simple software application, border crossing alert statistics as illustrated in Figure 5 are easily generated each day automatically, or interactively to give awareness to law enforcement personnel.

If border crossing alerts are also issued to the port of entry (POE) reporting stations, they can be cross-checked against vessel call-ins and used to identify those vessels who did not call in. Furthermore, with a real-time track display in the hands of call center personnel, call-in vessel operators can be questioned by telephone similar to land border POE questioning. For example, information about the vessel's current location, route of travel, time of border crossing, etc, can be logged and cross-checked against the radar tracks. Any suspicious behavior can be acted upon by the border agents (interdiction) and the intelligence analyst can be informed to trigger a more detailed analysis and/or an investigation. Even if border agents do not have the resources to interdict a suspicious call-in in real-time, the information obtained from increased questioning can be subsequently corroborated by radar data, providing a significant aid for intelligence gathering and investigations.

Additional intelligence can be gleaned in an analogous fashion (i.e. using a combination of real-time and target reach-back capabilities) by providing data persistence and user application infrastructure for Automatic Identification System (AIS) vessel track data. This cooperative track data can be mined in a similar manner as primary radar track data which tracks all targets, not just cooperating targets. Correlating AIS tracks with radar tracks allows identification of radar tracks to be made (via the AIS information) and provides additional indicators of suspicious activity. For example, we can determine if a vessel has turned off its AIS transponder, and track it thereafter.

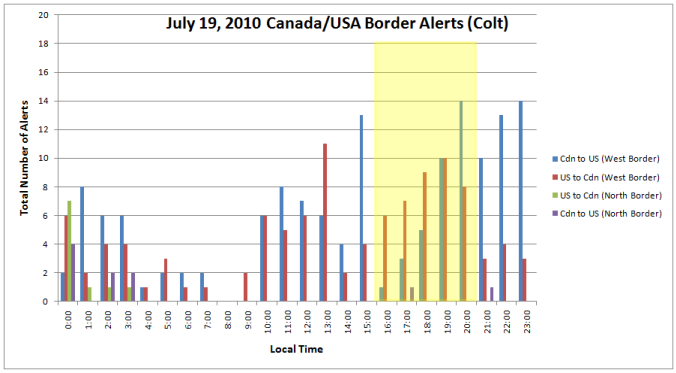

Figure 5. Border crossing alerts with direction by the hour.

Finally, intelligence-led border enforcement can also be supported with respect to low-flying aircraft. Radar information networks are used to track low-flying aircraft in the same way they track vessels; and Automatic Dependent Surveillance – Broadcast (ADS-B) cooperative tracks are used for aircraft in the same way that AIS is used for vessels.

In summary, automatically-generated border crossing alerts for vessels and low-flying aircraft derived from radar, AIS and ADS-B can be efficiently triaged by intelligence analysts with suitable user application infrastructure to improve security. In accordance with risk management principles, those TOIs with suspicious behavior can be passed on for further investigation.

Investigations. A variety of user software applications are available to support the work of investigators, following leads derived from the aforementioned radar and secondary surveillance (AIS, ADS-B and camera) information networks, or from other sources. Whereas the previous discussions focused on law enforcement actions associated with border crossings, investigations often focus on the origin or destination; i.e. on locations. With reference to the *there-and-back border crossing* example, investigations would be focused on the NY State marina and the Toronto waterfront property.

With data persistence and some rich, spatial/temporal query applications, we ask for information from the TIS such as the following:

1. Show me all of the target trajectories departing from or arriving at the Toronto waterfront location last night, last week, last month, or last year? (i.e. user-specified days/times)
2. Show me all of the target trajectories arriving at or departing from the NY State marine location during the same time period.
3. Filter the results by target size, maximum speed, behavior (e.g. steady speed indicative of sail boat or highly variable indicative of small pleasure-craft)

4. Cross-correlate the results to determine which subset of targets are likely the same, and the relationships, if any, between different targets.
5. Characterize the temporal distributions of departures and arrivals in support of future behavior prediction to drive planning and execution of covert operations
6. Link to other intelligence and investigative management software such as IBM's i2 to make additional connections between those who own, or operate from the locations in question.

The above investigative techniques can be carried out cooperatively with agencies on both sides of the border to first gain situational understanding, and then to ultimately detect and disrupt the cross-border criminal activity, resulting in arrests and seizures.

Prosecution. Prosecutors require evidence to support the burden of proof required for convictions. Given the vast waterways and airways over which cross-border criminal activity operates, and the different jurisdictions involved, the target reach-back data is critical to obtain the required evidence. Consider the case where the vessel leaving the NY State marina crosses well into Canada with a load of illegal cigarettes. The vessel realizes it is about to be pursued by Canadian law enforcement. It dumps the cigarettes into the lake and speedily heads back into US waters. Canadian officials pursue to the border, with one police vessel stopping to retrieve the dumped contraband. By the time the criminals are finally apprehended by cooperating US officials, their vessel is near the NY State marina. Target reach-back captures the entire scenario, with the criminal vessel's entire trajectory including the stoppage to dump the contraband and the police vessel's stoppage to retrieve it. Trajectory updates {lat, long, altitude (for aircraft), speed, heading, size) are date- and time-stamped and available every couple of seconds. This target data, along with the previous pattern of behavior captured by historical data that drove the investigation, serves as valuable evidence for the prosecution.

Management. Managers have the difficult task of applying their law enforcement resources in the most effective manner to reduce risk and enhance safety and security. Fortunately, with data persistence, the right user software applications can help tremendously with resource allocation. Consider Figure 6 which shows statistics on the west to east, US to Canada border crossings for the month of July 2010, based on radar border crossing alerts generated in accordance with the alerts shown in Figure 3. This report can be generated automatically with user software querying the TIS for border crossing alerts. In Figure 6, the results are filtered to only show small vessel border crossings. Each row represents the crossings for a given day in July, with the number of border crossings shown for each one-hour period in the day. UTC time (0 to 23 UTC) is indicated across the columns at the top, along with local time (2000 to 1900 EDT in this case) immediately below and highlighted in green. Each cell shows the number of border crossings (i.e. alerts) for the given hour generated by the radar information network. Cells with a greater number of border crossings are highlighted with a darker shade of red to quickly draw the manager's attention to the days/hours with the heaviest activity. The two most active periods of time are the 1st/4th July weekend (a national holiday in Canada and the United States) and 19 July when the sail boat race described earlier was taking place. Managers can use this data to allocate their marine units to particular border locations and times where they can be most effective. Year-over-year variations can be maintained for strategic planning. Daily variations can be used to make tactical adjustments as required. With a view of the entire Great Lakes system, for example, marine units from one area can be redeployed to another to maximize enforcement capability where the risk is greatest. Marine resource deployment can also be coordinated with land enforcement for real-time interdiction when a vessel is detected crossing the border and en route to a non-authorized location.

(/mm/yyyy)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	20	21	22	23	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
01/07/2010	0	0	0	0	1	1	0	1	0	0	0	0	1	1	0	2	0	0	0	1	0	1	1	0
02/07/2010	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	5	2	0	1	0	1	0	0
03/07/2010	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	2	1	4	4	0	0	0
04/07/2010	0	0	0	0	0	1	0	2	0	0	0	0	0	0	8	3	3	0	2	0	0	0	0	0
05/07/2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0
06/07/2010	2	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	0	0	0
07/07/2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1
08/07/2010	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15/07/2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	0
16/07/2010	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	2	0	0	0
17/07/2010	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0
18/07/2010	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	3	1	1	3	0	1	0	0	0
19/07/2010	0	1	4	2	2	2	0	3	1	2	1	0	0	2	6	2	7	9	2	4	2	4	6	2
20/07/2010	4	3	5	4	0	4	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	0
21/07/2010	0	0	0	0	0	1	0	0	0	1	0	2	0	0	0	0	1	0	0	0	2	0	0	0
22/07/2010	0	0	0	1	0	0	0	0	0	0	0	1	1	0	1	2	0	0	0	0	0	0	0	0
23/07/2010	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	1	1	0	0	0
24/07/2010	0	1	0	1	0	0	1	0	0	0	0	0	0	0	2	0	0	1	0	0	0	0	0	0
25/07/2010	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	2	1	0	0
26/07/2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0
27/07/2010	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0
28/07/2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
29/07/2010	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	5	2	0	0	0	0
30/07/2010	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1
31/07/2010	0	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	1	2	0	1	1	0

Figure 6. By the hour West USA to Canada crossings for July 2010.

III. TARGET INFORMATION SYSTEM DESIGN

The target information system is the heart of modern radar information networks [1,2] and the technical enabler for providing radar target integration, target data persistence and the user application infrastructure needed for the operational law enforcement capabilities presented in the last section.

The TIS design presented here is a practical design that has been implemented, tested and deployed operationally. A conceptual block diagram of a radar information network is shown in Figure 7. The TIS consists of the Target Database, Extended Database and Web Server components. The Radar Nodes provide surveillance and generate target tracks in their respective coverage volumes, sending these in real-time over the network to the Target Database. The Target Database relays this information to the Extended Database where it is reformatted, objectified, and where additional derived information is computed and organized for exploitation by users. Any number of users can interact with the TIS securely through the Web Server through which are available any number of user applications. User applications can also be deployed through local applications and clients as well.

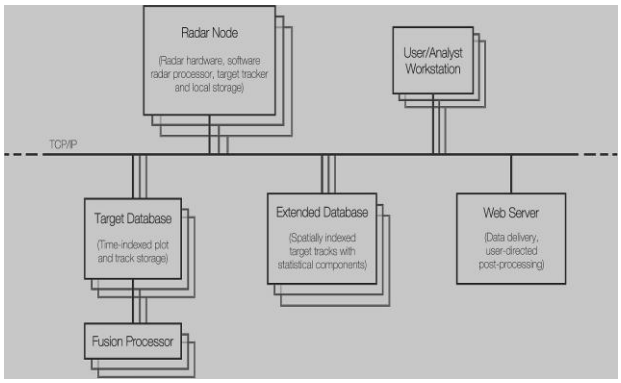

Figure 7. Conceptual block diagram of radar information network.

The technology supports an integrated, cross-border deployment strategy with an enormous cost efficiency, and full legal authority to operate.

The radar information network can be a completely private, secure network. Portions can also be shared securely with others consistent with their mandate. Components can be centralized, or they can be distributed inside different agencies. Any number of remote users can have direct, secure access to authorized timely information through the Web Server. User operational data can be contained behind their respective agency's firewall and segregated from *raw* radar track data. This allows agencies to share raw track data with each other in the same way that AIS or ADS-B data is open and can be shared. It supports unnecessary duplication in sensors and cost as stipulated by the Beyond The Border Agreement between Canada and the United States [3]. It further allows networks to be rolled out incrementally, with nodes "plugging into" the larger system on an ongoing basis.

The TIS is earth-centric and user-centric, not radar centric. All target data is in earth coordinates, and date and time stamped, allowing Radar Nodes to use dissimilar sensors which supports spiral upgrades and asynchronous interfaces between components.

The Target Database and Extended Database provide the target data persistence. They retain and organize target detection and track information continuously and permanently, updated every couple of seconds by the Radar Nodes. Storing all detections, as well as tracks, allows re-processing to be done after the fact which has proven to be extremely important in practice, especially for investigations. The Target Database is optimized for user applications that are time-driven, such as real-time displays, reviewing recorded target data, and reprocessing detections and track data (e.g. for fusion processing or for filtering on different target types). The Extended Database, on the other hand, serves for efficient searching and querying where spatial questions are being asked, such as those described earlier with respect to tools for investigations. The combination of the two databases allows arbitrary temporal/spatial questions to be asked of the TIS as needed for intelligence-led border enforcement. The various user applications desired for interdiction, intelligence, investigations, prosecution and management run as post-processors that query the Target Database and the Extended Database as needed to mine the target data and present it to the users requesting it.

IV. CONCLUSIONS

Through a discussion on border enforcement operations, we have illustrated that an eco-system of information products containing high-value intelligence and situational awareness is necessary to meet today's mission requirements. We have shown that with modern radar information networks, users involved in intelligence, interdiction, investigation, prosecution and resource management can all be readily served with the same investment, providing force multipliers and capability enhancements across the entire security enterprise.

Indeed, we have shown that with the right tools, we can triage small vessels and low-flying aircraft crossing unmanned borders between ports of entry to mitigate risk, in a cost-effective manner following risk management principles.

ACKNOWLEDGMENT

The author thanks law enforcement and national security personnel with the following agencies for numerous discussions over the past decade that have shaped the ideas presented herein: Royal Canadian Mounted Police, Michigan State Police, New York State Police, Canada Border Services Agency, Canada Coast Guard, US Coast Guard, US Border Patrol, US Department of Justice, Toronto Police Service, and the Niagara Regional Police. The author also thanks fellow engineers Sean Clifford, Graeme Jones, Carl Krasnor, Al Premji, Andrew Ukrainec, and Peter Weber, and special security advisor Scott Newark for their contributions and helpful conversations.

REFERENCES

[1] T.J. Nohara, "A commercial approach to successful persistent radar surveillance of sea, air and land along the northern border," 2010 IEEE International Conference on Technologies for Homeland Security, 8-10 November 2010, Waltham, MA.

[2] G. Jones and T.J. Nohara, "Wide area networks with data persistence", IEEE International Conference on Information Science Signa Processing and their Applications (ISSPA) 2012, 2-5 July 2012, Montreal, Canada.

[3] Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness, A declaration of the Prime Minister of Canada and the President of the United States, 4 February 2011, Washington, D.C..