The New Era of Security Risk Management
Table of Contents

Introduction ........................................... 2
The Adopt/Adapt Cycle ................................ 2
Flexible System Architectures ....................... 2
Realistic Field Verification .............................. 4
Avoiding Information Overload While Sharing Effectively . . 5
The Risk Management Lifecycle ....................... 7
Conclusion .................................................. 8
Footnotes .................................................... 8
Introduction

As governments have invested in security systems over the past decade, they have learned three pivotal lessons. First, as security technologies improve, adversaries continually adapt to defeat them; and, if a government’s security system cannot flex to address the altered threat, its value declines. Second, many technology or process solutions do not address the real-world conditions that operators actually face. Third, technologies designed to provide more information often overwhelm operators with data; so, rather than simplifying and speeding reaction, they actually can slow the response.

We are going to address each of these three challenges in some detail below, but first, it is important to emphasize that it is neither cost effective nor practical to try to eliminate all risks. Instead, we need to manage risks by considering which combination of threats, vulnerabilities and consequences yields the highest risk. The risk management life cycle described below can work to ensure that resources are properly deployed for optimal impact.

How can a government best prepare for and deal with the terrorist threat? Let’s answer this question by looking through the lenses provided by the pivotal lessons mentioned above.

The Adopt/Adapt Cycle

It is clear that our security forces and our adversaries are locked in a cycle – call it the Adopt/Adapt Cycle. When adversaries develop a new method of attack that addresses a vulnerability of ours, we develop a new countermeasure to defeat it. They then develop their next method of attack, and so forth. The speed of this cycle is fastest in the cyber domain. According to General James Cartwright, former Vice Chief of the U.S. Joint Chiefs of Staff, cyber attackers are adapting to improved security by developing their next attack tactic in as little as 9 to 14 days. For IED attacks in the war theater, attackers have adapted to new fuse defeating technologies in about 28 days.

To be resilient – that is, to be continuously effective despite an adaptive threat – a security system must be able to swiftly adopt changes to close vulnerabilities. We must analyze and discover how the attack works, develop or locate a sensor to warn when the attack is imminent, procure or develop that sensor, test it, integrate it with our CONOPS and our existing systems, and then deploy it. Any action we can take to speed the steps in this process will improve our resilience.

There are measures we can take to reduce the time and cost to adopt new countermeasures. These are: (1) build flexible system architectures; (2) conduct field verification before deployment, and (3) use adaptive analytics.

Flexible System Architectures

Security systems are best able to adapt to changed threats when they feature an open architecture and a completely modular design. An optimally flexible system would be built from independent, modular subsystems and components, interconnected by open standards-based interfaces both at the sensor-to- software interface, and at the software-to-software interface. In an open system, the internal structure of these subsystems/components is also modular and open-standards based. All of the system components should be built using commercial off-the-shelf (COTS) items, hosting software with commercial standard operating systems and infrastructure components, and interconnected by commodity networking components. This kind of architecture permits evolutionary development, new technology insertion, and competitive innovation. And, most important of all, a fast response to adopt improvements.
If this is our frame of reference, consider this: what would happen if security forces decided to rapidly add new border surveillance technologies in porous areas of the land or maritime borders -- would their security system incorporate those new sensors with relative speed and efficiency? Or consider that security forces might wish to deploy gunshot detection technology to alert on an armed assault on a port – would the system enable such technology to be incorporated quickly, and linked to cameras?

The “open” technologies that some vendors offer only operate within their own frameworks, limiting the user’s flexibility in the selection of hardware and software. Systems that limit hardware or software selection, or only provide interoperability within a proprietary interface, are in fact “closed”, rather than open to other vendor’s technologies. A system that cannot integrate new sensors without going back to the original vendor to have new software developed adds cost and delay to the effort. Such systems generally require support from the original vendor throughout their entire life cycle, which drives up the total cost. Over years of operation of the system, the customer’s opportunities for technology insertion are limited to only the R&D investments of the original system vendor, causing missed innovations made by the rest of the world. Even worse, the single vendor may eventually exit the marketplace, leaving customers stranded. All these drawbacks to monolithic and proprietary systems leave the security agency less resilient, less adaptive, and the nation facing higher risks.

It does not have to be this way. The development of industry standards and practices has evolved over the past 20 years. The net effect has been to open up applications and facilitate interoperability, accessibility, and extensibility among applications. This has lowered both costs and risks for customers of security products. The strategic imperative for a security agency is to demand open and modular architectures.

To determine whether a vendor is describing an adaptive system, it is advisable to look for:

- The quantity and quality of exposed interfaces;
- Service functionality and service interfaces;
- Standards employed for interface definition and messaging;
- Software Development Kit (SDK) and software Application Programmer Interface (API) availability, ease of use, completeness and documentation;
- The degree of software interdependencies with other products (if any exist);
- Backwards compatibility with previous application versions;
- The ability to add and operate system components from other makers, such as sensors, radios, or analytical engines such as trackers or automated threat recognition; and
- The time and level of effort required, in a live test, to add a system component from an independent vendor to the system.

These open architecture principles apply to a system of systems, such as an integrated border surveillance system that consists of sensors, platforms, command & control software, and response forces; or if we are evaluating a single sensor, such as a baggage screening sensor. Sensors that have open standard interfaces and segregate their signal processing into a module are more resilient to threat migration because they can be constantly updated, and can benefit from the “app store” model – from innovations developed by other businesses, without having to replace the entire sensor.

A closed, proprietary baggage screening sensor relies solely on the maker to develop improvements and innovations, but an open screening platform allows the world of technologists to develop positive changes. An open, modular baggage screening system would have the image analysis module separate from the hardware, enabling the owner to plug and play other analytical modules. If that module had an open
interface, the operator could upgrade it with algorithms from third parties. Most importantly, with an open analytical module, new threat intelligence could lead to changes in automated threat recognition, learning algorithms, advanced risk assessment and graded screening rules, and operator defined rules for screening intensity.

Other examples of sensors that, if open and modular, would be more resilient include:

- Whole body imagers
- Nonintrusive vehicle and cargo screening
- Traveler and visitor management systems
- Access control systems
- Insider threat monitoring systems

With an adaptive and open architecture as the core of a security surveillance and response system – whether for borders, maritime, urban security, aviation, immigration, transportation, or critical infrastructure – the possibilities for sensing threats are immediately expanded to all sensors available today and tomorrow. Consider urban security. Today most cities rely on a network of cameras to support situational awareness, enhanced response and evidence collection. With an open architecture C4I system, security personnel get far more than sight. Sensors available today and coming soon can be networked to detect gunshots; radiological, chemical or biological weapons; explosives; deteriorating infrastructure; and threatened underground pipelines. And, with new signal processing and tracking capabilities, operators will not simply receive alarms, but get photography and license plate numbers linked to the triggering entity and be able to track that entity as it moves until interception.

The adaptive, resilient architecture we are describing here directly affects the security agency’s ability to win in the adapt/adopt cycle. So, in summary, here is what this adaptive architecture gives us:

- Improved operational performance with plug and play sensors selected to adapt to the threat, and not restricted by interface design or compatibility with previous purchases;
- Maximum flexibility allowing for easy reconfiguration to support new tools, sensors, or changed conditions;
- Maximum independence by allowing the freedom and ability to make changes to the system without relying on any particular manufacturer. The operator agency should have the freedom to change workflows and to add and remove sensors or software modules without engaging the original vendor; and
- Maximum mobility enabling unpredictability in the agency’s concept of operations. A system that can be efficiently reconfigured or disassembled and moved to another location allows government to act on new intelligence information and to be less predictable to opponents, a deterrent effect.

Realistic Field Verification

Let’s now focus on our second pivotal issue – whether our technologies are keyed properly to real world conditions. To be useful, technology must work, not just in a lab, but in the actual operating environment in which it will be used. Unfortunately, we have seen many technology or process efforts that do not reflect operational reality. For example:

- U.S. efforts to deploy persistent surveillance on the southern border have encountered numerous challenges in the diverse environment of Arizona. Early in a project (which was called SBInet), newly deployed radars interpreted rain or other natural phenomena as alertable events, making the system unusable³.
Similarly, the U.S. launched a major effort several years ago to conduct background checks for all port workers, requiring them to use tamper-resistant credentials as a condition of entering a port facility. While such credentials have been issued to more than one million port workers, authorities have struggled to find card readers that will operate efficiently in a port environment so as to minimize delays at port entrances. During pilot tests in 2006, port authorities who installed readers in the outdoor maritime environment concluded that their poor performance was due to damage by dirt, wind, salt, and water.

Expensive camera systems have embarrassed police by failing to capture serious crimes committed in full view, and costly gunshot detection systems have failed to record nearby shooting homicides.

To avoid similar failures, it is vital, when considering new technologies, to learn: how they will perform in the environments where they will be deployed; how they will actually be used; and how an adversary will attempt to defeat them. Proper field verification requires building an operational test environment identical to the field where a new system is to be deployed – that is, on the coast, on the border, in the airport, etc. This provides a stage where systems can be evaluated and operated as they will eventually be used.

In such a test environment, actual operators can use the system and provide feedback for adjustments to help the maker to get it right, and build buy-in to the final product by the users.

In a proper environment, sensors can be tested to determine actual performance in conditions identical to where they will be used. Systems integrators and customers have found substantial differences between the performance claimed by sensor makers and that actually achieved. When this difference is known in advance, the system's design can be adjusted accordingly. When discovered after deployment, the costs and consequences can be unacceptable.

In a realistic test environment, an independent agency may be tasked to act as a red team and attempt to defeat the system. In this way, system vulnerabilities may be identified and addressed.

Avoiding Information Overload While Sharing Effectively

More sensors collecting more data is no sure way to mitigate threats. We know that some solutions intended to create “walls of knowledge” for security officers have, in fact, created “walls of confusion,” overwhelming them with feeds from cameras, sensors and multiple databases. Security personnel have a limited capacity to process and act on data, no matter how highly trained they are. Technologies in signal processing, adaptive analytics, and secure information sharing can be leveraged to ease the burden on security personnel, to free “humans to do what they do well: think, ask questions and make judgments about complex situations.”

Here are examples of such technologies:

A Multi-Hypothesis Tracker (MHT) can process real-time signal data from hundreds of heterogeneous sensors like radars, cameras, geo-located unattended ground sensors, video analytics, blue force tracking transponders, and sensors on aircraft, aerostats, mobile sensor systems, and remote video surveillance systems – if necessary all at the same time – and produce from the clutter single tracks for all targets. With an MHT, a C4I system can display that target with its heading and speed on a GIS display; automatically point a camera onto that target to enable identification and classification and keep it in view as it moves; and continuously maintain that track and its history as long as the target is within range of any sensor. Specific versions of MHTs are available for marine targets and ground targets.

As a core element of a surveillance C4I system, an MHT reduces operator workload by eliminating spurious reports and “connecting the dots” of sensor observations over time. The MHT allows operators to see the events unfold in the area of interest without being overwhelmed by the number of reports being presented. An MHT is key to adaptive resilience and operator efficiency because it
removes the white noise of singular, unique alarms, such as those from wind or animals, by not presenting events unless a track with the right characteristics is resolved from across multiple sensor types. The MHT increases effectiveness of response by enabling an operator to guide response right to the moving target.

- A C4I system that includes doctrine-based alerting can greatly improve the ability of operators to discern which, among potentially hundreds of targets, represent the greatest risk, thus ensuring response forces are focused on the most likely targets. As implied in the name, this module of a C4I system is configured to alert on the basis of triggers defined by its operators. Many C4I systems enable the operator to designate a certain area of operations as sensitive so that any entries to that area trigger an alarm. Doctrine-based alerting goes farther by using behavioral analytics so that factors such as track history, speed, bearing, changes in speed or bearing, and the convergence and/or separation of targets, are constantly analyzed to produce a dynamic risk score for all detected targets. This capability is particularly necessary when the challenge is to detect a threat as soon as possible when the environment is cluttered with a lot of “friendlies”, as in a port or on fishing grounds.

By employing user-defined rules, operators can prompt data systems to generate real-time warnings automatically when new information is collected that matches the operator’s criteria, without the operator having to view all the new data. Queries can also look backwards in time for instances that match the same criteria.

- A single individual may have multiple encounters with different security or law enforcement agencies over time. Each encounter may initially appear inconclusive, but the encounters may – when considered together – indicate a more significant threat. Successfully linking identities in different records has proved historically challenging. Problems in biographic identity resolution have led both to undue delays for innocent civilians and missed detections of high-risk travelers.

Innocent errors in name-matching, combined with criminals’ frequent use of aliases, highlight the vulnerabilities in identity assurance. Multilateral immigration data sharing initiatives have revealed significant amounts of potential fraud in the asylum process. The solution is an integrated set of analytical tools for entity resolution that reach across agencies’ databases to compare biographic data on a person using rules and algorithms, fuse the right information into a single identity, and then ideally link this to biometric data on the person. Biometric data have proven critical in identifying terrorists seeking to subvert the refugee processing system to infiltrate target countries.

Multiple software and hardware systems are available for biographic and biometric applications, but tradeoff analyses are required to determine which combination of tools is best suited for a given setting.

- Interoperable data sets – whether biographic or biometric – are key identity assurance enablers. A number of agencies may store information relevant to an individual’s identity, but have no means of cross-checking or consolidating that data. Indeed, some of the most significant gaps in identity management relate not to the lack of identity management systems, but to gaps in connectivity between government agencies. Challenges to interoperability can be both policy and technical. Establishing trust among data system owners is a precondition to effective interoperability and information sharing. Data owners need to have confidence that their data is going to be appropriately handled. Audit and policy violation detection tools should be in place to minimize potential for misuse, and privacy and confidentiality protections should be built into the system architecture so that the only people who see the data are those who are supposed to see it – and only when they are supposed to.
From a technical and standards point of view, interoperability can be a complex effort. Semantic interoperability standards allow two databases to talk to each other; but technical interoperability know-how is what you need to map one dataset to another, particularly at scale. Both are necessary so that information can flow easily from one system to another and be understood. An automobile may be called a “car” in one database and a “vehicle” in another. Interoperability standards and know-how are key building blocks that enable information sharing.

A corollary to the use of COTS and standard technologies is that the vulnerabilities inherent in these products are shared. The exchange of cyber threat data and the rapid adoption of fixes to cyber gaps are critical. When the gaps are known, the adversary can exploit them. When a new vulnerability is discovered in an attack on one target, the methods of the attack and the way to fix them should be shared will all other users. Ninety-three percent of successful cyber security attacks exploited known, publicly announced vulnerabilities for which fixes had been issued by vendors, but just not applied by users. Therefore, sharing data on successful attacks, and simple good hygiene in applying the fixes, will dramatically reduce cyber vulnerabilities at the same time as they increase the adversary’s costs. Secure, structured information sharing environments can be applied to enable sharing intelligence from a successful attack without divulging the victim.

Strong technical expertise in sensor signal processing, as well as integration of COTS analytics products, can help ensure an effective implementation of information analysis and interoperability systems. However, such expertise must be coupled with domain expertise in the nuances of the data in question, as well as privacy and confidentiality imperatives for circumstances where data will be shared among multiple agencies.

The Risk Management Lifecycle

Having examined these critical lessons learned, it is appropriate to turn to the most generic topic of all in the realm of counterterrorism: how to manage the risks. Here are the steps in this all important process.

**STEP 1 – Intelligence and Information Sharing.** All source intelligence on threats is collected and securely shared across agencies and with the security forces of targets.

**STEP 2 – Threat & Vulnerability Assessment.** Given intelligence on intended attack targets, means and methods, a threat and vulnerability assessment is conducted to identify vulnerabilities to the attack, including in the physical, cyber, and identity domains. Risk prioritization models are used to weigh the probability of attack, the identified vulnerabilities, and the consequences of a successful attack in order to determine where to focus improvement activities. A design-basis threat is then produced to document the problem to be addressed with improvement activities.

**STEP 3 – Modeling & Simulation of Alternatives.** Modeling and simulation (M&S) software programs are a significant aide to governments that are taking stock of their existing security enterprise and seeking to improve it. With open models (meaning, models in which logic, assumptions and variables can be very easily changed to improve fidelity of the model), agencies can study or game strategy, processes, manpower, sensors, software, infrastructure, and the positioning of all these resources for maximum deterrence and responsiveness. The range of options has a range of costs, so the challenge is to choose those changes that most cost effectively reduce risks. With M&S, different blends of capabilities can be compared against one another in different operational concepts and constructs. During the planning and solution design process, M&S helps operators understand the environment and the capabilities and limitations of technology and other resources by providing a virtual world in which to experiment with options prior to actual deployment — well before funding and resource commitments are made. M&S can also help planners explore different response models
needed to confront a given threat. M&S offers a disciplined look at problems that can save money (we do not buy equipment we do not need) and time (we reach a common understanding of our challenges faster). This produces a conceptual solution.

**STEP 4** – Concept of Operations. The conceptual solution design is converted into a concept of operations (CONOPS). The CONOPS is a blend of technological, physical, and human components formed into an optimized solution; it includes a recommended architecture of processes, sensors, software, information technology, and tactical infrastructure. A CONOPS is ideally accompanied by a recommended staging of security changes that account for readiness of security forces to absorb change, and the government’s ability to fund programs. In this step, mission experts define the specific procedural changes that will be implemented with the new CONOPS, including the introduction of any new strategies, technologies, manpower, or infrastructure. This step also includes any procurement and the integration of a system prototype.

**STEP 5** – Field Trials. With the system prototypes built, we test them in a realistic environment. Depending upon the change being implemented, red team testing may also occur.

**STEP 6** – Implementation. Implementation is where the solution becomes tangible. During implementation, roll-out principles such as piloting, phased implementation, adaptive response, and process measurement guide the overall implementation plan.

The planning process does not end at implementation; it begins a new cycle. Planners will collect the metrics that were established during the planning phases, measure these in actual operation, and evaluate the degree to which the plan is succeeding. The evaluation and analysis of the effort may result in changes in the strategy, adjustments in tactics, and/or the establishment of updated goals. Given constant vigilance and intelligence collection, the risk management life cycle will kick-off again whenever new intelligence on threats is received, accelerating the agency’s adoption of countermeasures to the adaptive threat.

**Conclusion**

In the material above, we examined three of the most common and serious challenges facing nations’ counterterrorism experts: coping with the Adopt/Adapt cycle; effecting realistic testing of concepts and equipment; and managing the information explosion in the field. Our conclusion is that there is promise within reach in all areas. Finally, in closing, we reexamined the critical process for analytical risk management which, if performed well, is the key to our problems.

**Footnotes**

1 George Washington University Homeland Security Policy Institute, Capstone Series on Cyber Strategy; General James Cartwright (USMC retired), former Vice Chief of the US Joint Chiefs of Staff, May 14, 2012.

2 Ibid.


For example, Rafael Resendez-Ramirez, an immigration absconder wanted by the FBI for numerous murders, routinely used aliases. The lack of interoperability between border authorities and the FBI led to his mistaken release from Border Patrol custody. See U.S. Department of Justice Office of Inspector General Special Report: The Rafael Resendez-Ramirez Case: A Review of INS’s Actions and the Operation of Its IDENT Automated Fingerprint Identification System, March 20, 2000, Section 5.

Supra, note 1.