NATO OTAN NURC

a NATO Research Centre
un Centre de Recherche de l'OTAN

NURC
PARTNERING FOR MARITIME INNOVATION

Reprint Series **NURC-PR-2008-008**

Security versus defence: dual use from a system requirement perspective

Ronald T. Kessel

September 2008

Originally published in:

Proceedings of the 1st International Conference and Exhibition on Waterside Security (WSS 2008), Technical University of Denmark, Copenhagen, Denmark, 25-28 August 2008.

About NURC

Our vision

- To conduct maritime research and develop products in support of NATO's maritime operational and transformational requirements.
- To be the first port of call for NATO's maritime research needs through our own expertise, particularly in the undersea domain, and that of our many partners in research and technology.

One of three research and technology organisations in NATO, NURC conducts maritime research in support of NATO's operational and transformation requirements. Reporting to the Supreme Allied Commander, Transformation and under the guidance of the NATO Conference of National Armaments Directors and the NATO Military Committee, our focus is on the undersea domain and on solutions to maritime security problems.

The Scientific Committee of National Representatives, membership of which is open to all NATO nations, provides scientific guidance to NURC and the Supreme Allied Commander Transformation.

NURC is funded through NATO common funds and respond explicitly to NATO's common requirements. Our plans and operations are extensively and regularly reviewed by outside bodies including peer review of the science and technology, independent national expert oversight, review of proposed deliverables by military user authorities, and independent business process certification.

NOTE: The NURC Reprint series reprints papers and articles published by NURC authors in the open literature as an effort to widely disseminate NURC products. Users should cite the original article where possible.

SECURITY VERSUS DEFENCE: DUAL USE FROM A SYSTEM REQUIREMENT PERSPECTIVE

Ronald Kessel[a],

[a]NATO Undersea Research Centre, Viale San Bartolomeo 400, La Spezia 19126, Italy

Ronald T Kessel, NATO Undersea Research Centre, Viale San Bartolomeo 400, La Spezia 19126, Italy, Phone: +39 0187 527 248, Fax: +39 0187 527 331; E-mail: Kessel@nurc.nato.int

Abstract: *The developers of defence technologies in both industry and national laboratories have naturally carried their culture for military system development into the evolving security mission, even for systems that are to be used by civilian security personnel. There may be fundamental differences, however, along the way from threat analysis to plausible modes of response to system requirements; differences that lead to a mismatch between the technical solutions that are being proposed and the new customer's interest in them. Hurdles to an immediate transition are to be expected in any enterprise that moves to serve a new customer base. This paper attempts to identify changes of emphasis that can impede the dual use—military and civilian—of the security solutions proposed by developers.*

Keywords: *Port Protection, Dual-Use, Technology Transition, Counter Terrorism, System Development, Marketing*

1. MORE THAN "TARGETS"

It is safe to say that in waterside security virtually all human activity in the area of interest—in the operating picture—will be legitimate, or at least benign; otherwise we would not be dealing with terrorism but with a widespread militant revolution of sorts. Port authorities may therefore be a little amused when defence developers, while discussing port protection in the literature, at a conference, or during system demonstrations, repeatedly refer to contacts in the operating picture as "targets". A genuine target should be very rare in practice though the operating picture is full of human activity day after day. People going about their daily business in a port would also feel uncomfortable, perhaps alarmed, to discover that someone looking at the operating picture may be referring to them as a "target". This discomfort may or may not be a good thing. It may be an inevitable or essential part of security, contributing to vigilance and order on the one hand, and to the betrayal or deterrence of attackers on the other. At the same time, however, the twinge of novelty or discomfort with "target" may be a clue that defence developers are not thinking correctly about security; that there may be a mismatch between the starting points—the anchoring concepts—adopted for new systems by defence developers and those required by security providers.

Needless to say, the premise behind much of military countermeasures is that a particular mode of attack is underway, and that the system is expressly designed to stop that mode of attack. The initial and long-term costs of the system pay off above all if the threat materializes into an identifiable attacker (the "target") and the system succeeds in stopping the attack. So much is obvious. At first glance the same transfers immediately to security. But there are differences between military combat and security, and these differences can become points of resistance to system procurement and funding when defence developers try to make a switch from one market to the other. These differences are considered here.

The premise behind much of security in counter terrorism, roughly stated, is that there are attackers somewhere in the world who are intent on attacking somewhere, and that security measures (systems, regulations, and so forth) are designed to stop them. The "threat" is the expectation of attack [1], and not a particular contact in a scene as developers often have it. The port goes about its regular business with its operating picture populated entirely by legitimate contacts to which a set of meaningful labels applies—particular ship or industry names, or more generally classes objects such as "fishing boat", "recreational craft", "passenger carrier", "tugboat", "ferry", "garbage handler", and so forth. It is from out of this context that the business of waterside security generally operates. One speaks moreover of "unauthorized entries", a "contact of interest", behavioural "anomalies", hazardous goods, and so forth, but rarely of "targets".

More than semantics are at issue. It would be easy enough to add a rarely used "target" label to the set because, as the technical literature everywhere suggests, any maritime contact might conceivably prove to be a terrorist attacker. But in practice the "target" label means nothing if it does not signal a dramatic change of stance and response toward a contact. It signals that one has judged a contact to be very dangerous and that it must be stopped, with force if necessary, through actions that may themselves pose considerable risk. Yet in practice the "target" designation is a difficult call to make. It is likely that the attacker will not be easily identifiable as such. They will pass instead as legitimate activity in the port until the final moments of attack. Their clothes and equipment will be that of others commonly seen. One looks therefore for proof of intent, by detecting weapons or

explosives in a spot check perhaps, or, more typically in waterside security, from noncompliance in the face of warnings, barriers, or nonlethal stopping measures, and so forth. One also hopes at the same time for detailed prior intelligence of high certainty, from investigative police work or tips.

The "target" label can also be problematic in military combat, especially in asymmetric warfare. As a rule, however, in combat between states the combatants and their weapon systems are for the most part identifiable to each other once seen, whether visually or by remote imaging, and this visual-quality identification at once initiates and justifies the "target" designation, and does so with fairly high certainty. In many military operations other than war the situation more closely approximates security, and calls for different operational and system planning along the lines sketched below.

2. JUSTIFICATION, UTILITY, AND CONSENSUS

The elevation of a benign contact to a "target" implies that a dramatic uncertainty reduction (information gain) has taken place regarding one or more contacts in the operating picture of the port. The means for producing this information comprises much of the work of security. Security and its methods properly assure that cues to hostile intent are available when they are required. When system developers speak of a "target", however, they enter the stage after information about intent has been acquired; that is, after much of the work of security—the discovery or forcing of cues to hostile intent—has already been done. Indeed, the supposition that a system designed for "targets" is helpful to security providers falls into question. For if genuine targets are rare, then the system's utility will rarely if ever be realized at a particular installation. Indeed, the justification of the system can hardly be made on the basis of its overall utility to security providers. It will be a burden, demanding additional expertise, expense, and vigilance. Judging from the technical literature (see the literature survey in [2]), the justification for the system really does not come from its utility to security providers in their daily work at all. It comes rather from the high cost of the consequences of an attack—that is, the potential loss of life, economic impact, environmental destruction, and so forth. This justification is why system developers usually begin their articles and presentations with a cursory risk analysis of sorts, painting a picture especially of the consequences that an attack may have. The prospect of assisting in the daily work and complexity of security is scarcely cited as a requirement. Though not intending to increase the work and complexity of security, this is what would typically happen.

Justification of a new protection system on the grounds of the serious consequences of an attack has its merit, of course. One rationally defends against rare critical events if their consequences would be unbearable. At the same time, however, one is not catering very directly to the security provider this way. The security provider faces the burden of supporting an additional, very complex system, with only a remote potential payoff in the rare event of an attack. That additional burden may be worth it—, or it may not. It is difficult to make a convincing case with broad appeal either way. This is because the argument, whether pro or con, amounts to a risk analysis applied with a particular mode of terrorist attack in mind, and at just those sites where the system is to be installed. The risk analysis is carried out at best by experts, amid much uncertainty (the "deep" uncertainty of terrorism as some say [1]), and with high variability from place to place and from time to time. At worst the risk analysis amounts at worst to personal guesses about the terrorist threat and capability. In any case, the risk analyses generate more debate than consensus among experts and non-experts alike, especially if the new system is expensive. A strong

consensus about system utility is nevertheless required to carry the day if a large investment is to be made. Despite the sense of urgency regarding counter terrorism, developers therefore have difficulty finding buyers for their new systems. The impetus that the high consequences of an attack at a site might have had to forge consensus to invest in a protection system is undermined by the fact that the likelihood of attack at any given site is generally low and uncertain, so other grounds for consensus are required.

3. ALTERNATIVE PERSPECTIVES

One of the primary motivators behind security providers is of course their mandate as defined through legislation and obligatory regulations. In them one finds the stakeholders in security such as they really are, and not as developers imagine them to be. To give just one example, for ship and port facilities the most general marching orders toward new security measures has been the ISPS code [3]. In the ISPS code one finds constant motivation that is almost beyond question, as opposed to the subjective, changeable, uncertain perceptions of risk that developers rely on most. Security providers on ships and in ports can be expected to do as much as these and other regulations require.

The mandate and regulations followed by security providers generally changes from country to country, and from jurisdiction to jurisdiction within a country. If strong links can be made between a security provider's mandate and the protection offered by a particular system, then it will be a more convincing route for transitioning and marketing new systems. Consensus can be taken for granted, reducing marketing to a question of which system rather than whether or not a system is necessary in the first place.

Mandates and regulations are always changing, of course. It is necessary to keep abreast and, if possible, to shape their direction by new innovations. The Automatic Identification System (AIS) for ships, originally intended for collision avoidance but now used for security as well, and required now by the ISPS code, is an example of new technology influencing regulations. Its dual safety and security use is a clear selling feature. The case of AIS may serve as a model for other new protection systems in waterside security and warrants further study.

Elsewhere the case for new protection systems might be made to shipping companies and port facilities on business grounds as well, not only through the consequences of a successful attack, but through reduced insurance costs [4], reduced theft [5], better service delivery for customers (through better control), or through favoured status that might result from new equipment. We cannot go further into these possibilities here. The general points to be made, rather, are 1) that there may be very good grounds for purchasing new protection systems other than the consequences of a very rare but successful attack, 2) systems that find utility more immediately in daily reward more easily win the consensus that large investments typically require, and 3) the systems promising daily utility are likely to be very different than the military-style systems that defence developers have been proposing.

If we keep to the military-style protection systems designed for stopping an attack during the moments that it is underway, then the need for obvious utility and winning consensus constitute top-down system requirements of sorts. The system must itself force cues to hostile intent to the surface, or it must fill a role in a larger system of systems that forces proof of hostile intent by other means. There is unfortunately no sensor for measuring hostile intent from a distance, but it can often be plausibly assessed nonetheless, by observing noncompliance in the face of unambiguous warnings, barriers, or other nonlethal deterrents. Unauthorized entries might first be warned away by

unambiguous markers, barriers, or audible signals; they might be identified by near visual quality imaging, to be observed for a time for noncompliance as warnings are made more explicit and energetic, and to be assured that compliance is possible; they might be subjected to increasing discomfort by nonlethal means (projected energy—light, sound, electromagnetic pulse or beam); and so forth.

It is when system developers begin thinking along these lines, and not when they think of the consequences of an attack, that they enter into the work of security. Developers are beginning to appreciate the need for proof of intent, but it remains a secondary consideration, as an after thought when much of the protection system has already been designed rather than as an essential part of the new system itself, as if it were another's concern. When transitioning military technology into security, rather, it is necessary to give equal consideration to three correlated dimensions at once: to surveillance, to proof and discovery of hostile intent, and to response.

4. TECHNOLOGY TRANSITION

It is clear that the "target" label is too strong for much of security, even in counter terrorism. When we stop to consider what exactly is meant by "target" we begin to face the challenges of security squarely, with implications for system design and utility. We then begin to deal with "unauthorized entries", "barrier breach", behavioural "anomalies", and actionable intelligence tips on the one hand, and with proof of intent, and progressive graded-level response on the other; all of which are much more the daily work of security providers. To elaborate on these requires specific knowledge of a particular security provider's mandate, daily operations, and rules of engagement, which cannot be taken up here. More generally, by dropping the "target" label the challenges of security are faced much more from the security provider's perspective, and the prospect for meeting the security provider's needs improves. This is a marketing approach of sorts toward system development, working systematically from customer needs and problem definition, to solution.

Unseating the "target" label also calls for new or modified system metrics. In military surveillance systems, for example, the single most important metric may be the *probability of detection*—the probability of registering the approach of a particular class of "targets" given that one such "target" is in fact approaching within the field of view. In response to a target, on the other hand, there is the *halt probability*—the probability of stopping a target's advance at a safe distance, given that a target is advancing. These metrics serve as drivers in the design process, in operations research, in technology selection, and in making many of the countless engineering tradeoffs that complex systems inevitably require. Their utility cannot be disputed, for only when under attack does a defence system prove itself, but they enter the security stage after the matter of target designation has already been settled and therefore miss the foremost challenges of security. What emerges is a system designed and selected for a caricature of the security operating picture. Contacts are subdivided into just two classes: into targets on the one hand (admittedly rare and uncertain but of an extremely critical nature), and into false alarms on the other (very common and of little interest). This duality properly drives much of defence-system thinking and operation, but it is generally mismatched with security whose operating picture is populated by many contacts that are worthy of note though they are neither targets nor false alarms. Metrics that touch more directly on target designation through proof of intent are required. Here again, when thinking about the kinds of metrics that

should be used for security, one departs from military combat and enters more directly into the work of security.

In this regard it is useful return again to the premise behind security given earlier: that there are attackers somewhere in the world who are intent on attacking somewhere and that the security measures are designed to stop them. This premise opens the door to other modes of system effectiveness. The developer's new system may function, for example, along two different fronts at once: by 1) stopping an attack that is underway, and 2) by deterring attackers from attempting an attack where the system may be operating. It has been said that deterrence functions as a 2 to 10 times force multiplier in security [6]. This was in turn given some quantitative game-theoretic justification in [7] provided that one allows the attacker to shift his or her targets. In any case, the developer's system can be expected to deliver more real stopping effect than quantified through system technical evaluations through human factors of deterrence. Deterrence is a valid stopping force, especially for security operations, but it is typically omitted by defence developers owing to the presumption that an attack is already underway. The prospect of such a force multiplier is of considerable interest, especially if its effect could be estimated and incorporated into a larger risk analysis and business case for new systems.

By allowing for the entry of deterrence, moreover, one counters somewhat the doubts often raised about ostensibly lower-level, more affordable, more sustainable measures that security providers already provide and naturally gravitate toward. Although such measures might in some places be defeated in ways that a non-expert can imagine, they are not for that reason irresponsible or to be dismissed. Their effectiveness can be much greater than they first appear from a military combat perspective. Deterrence is not an argument for complacency in system developers. They are still obliged to design the best affordable systems because the deterrence comes after all from the expected effectiveness in the event of an attack.

5. CONCLUSIONS

Although the military may be called upon for security operations in counter terrorism, it does not follow that military systems will therefore transition directly into security operations such as port protection. There is still a requirement that the systems should appear obviously useful to security providers who are expected to buy and operate them. An appeal to the high consequences of an attack is inadequate because on its own its force depends entirely on the likelihood of attack, which is endlessly debatable given the "deep" uncertainty that characterises counter terrorism, and which therefore cannot garner the widespread consensus that large capital investments typically require. Other parallel lines for system utility must be found along much more certain ground, in the mandate and regulations of security providers, in a business case for industry, in alternate modes of effectiveness (like deterrence), and so forth. When adopted as system drivers, these are likely to produce rather different systems than the systems now being proposed by defence developers.

More particularly, for systems that are intended to stop an attack during the final moments that it is underway, the point of departure from military combat and the point of entry into security lie in the requirement for proof of hostile intent, and in the discovery of hostile intent. This daily work of security must be viewed as an integral part of stopping action, integral to system design, if the system is to feature in a coherent vision for security operations and win the consensus required for large capital investments.

REFERENCES

[1] **H. Willis, A. Morral, T. Kelly,** and **J. Medby**, *Estimating Terrorism Risk*, RAND Centre for Terrorism and Risk Management Policy, RAND Corporation, 2005.
[2] **R. Kessel**, Protection in Ports: Countering underwater Intruders, *Proc. of Underwater Defence Technology (UDT) Europe 2007*, Naples, June 2007.
[3] Guidance for Ship Operators on the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code, International Chamber of Shipping (ICS), London, 2003.
[4] **P. Donner,** Maritime Insurance for Piracy or Terrorism – Drawing a Line in Water, Strategic Insights, No. 10, pp. 19-23, March 2008.
[5] **Market Access International**, U.S. Port Safety and Security Survey Report, Homeland Defence Journal, Special Publication, Feb 2007.
[6] **R. Anthony**, An Empirical Model of the Psychology of Deterrence: Reality Does Not Conform to Theory, *National Institute of Statistical Sciences Workshop on Statistics and Counterterrorism*, 20 Nov 2004 (Internet Publication http://www.niss.org/affiliates/wsc112004/speakers.html#anthony, last accessed 10-April-2008)
[7] **R. Kessel,** Deterrence as force multiplier in port protection and the defence against terrorism, NATO Undersea Research Centre Full Report, NURC-FR-2008-015, May 2008.

Document Data Sheet

Security Classification		Project No.
Document Serial No. NURC-PR-2008-008	Date of Issue September 2008	Total Pages 7 pp.

Author(s)

Kessel, R.T.

Title

Security versus defence: dual use from a system requirement perspective

Abstract

Keywords

Issuing Organization

NURC
Viale San Bartolomeo 400, 19126 La Spezia, Italy

[From N. America:
NURC
(New York) APO AE 09613-5000]

Tel: +39 0187 527 361
Fax:+39 0187 527 700

E-mail: library@nurc.nato.int