From Strategic Security Risks to National Capability Priorities

Rick Nunes-Vaz, Steven Lord and Daniel Bilusich

Since 9/11, many western nations have re-framed their national security decisions in terms of strategic risk management. All have undertaken risk assessments, but valid translation into capability priorities has been abdicated largely by transferring priorities directly from risk magnitudes. Treatment priorities should be determined from risk reduction benefits in relation to costs, but a method for assessing risk reduction effects has been broadly elusive. This article shows, in a pragmatic way, how treatment options are generated, and how the capabilities that contribute most to risk reduction can be identified. These should be priority targets for the investment of limited resources.

Over the last ten years many western nations, for example, the United Kingdom,[1] Canada,[2] the Netherlands,[3] the United States[4] and Australia,[5] have adopted risk as a central part of their national security decision-making and prioritisation. Each has initiated a process of strategic national security risk assessment[6] that feeds and informs discussions on capability priorities, in turn, informing resource allocation decisions.[7] There has been

[1] UK Government, *The National Security Strategy of the United Kingdom: Security in an Interdependent World* (Norwich, UK: Cabinet Office, 2008); UK Government, The *National Security Strategy of the United Kingdom: A Strong Britain in an Age of Uncertainty* (Norwich, UK: Cabinet Office, 2010).
[2] Canadian Government, *Canada's National Security Policy: Securing an Open Society* (Ottawa: Privy Council Office, 2004).
[3] Netherlands Government, *National Security: Strategy and Work Programme 2007-2008* (The Hague: Ministry of the Interior and Kingdom Relations, 2007).
[4] US Government, *The National Strategy for Homeland Security* (Washington DC: Homeland Security Council (US), 2007).
[5] Attorney-General's Department, *Guide to Australia's National Security Capability* (Barton, ACT: Commonwealth of Australia, Attorney-General's Department, 2013).
[6] For example, Cabinet Office, *National Risk Register of Civil Emergencies: 2012 Edition* (London: Cabinet Office, UK Government, 2012); Department of Homeland Security, *The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation* (Washington, DC: Department of Homeland Security, US Government, 2011); Analistennetwerk Nationale Veiligheid, *Nationale Risicobeoordeling* (Bilthoven, Netherlands: Rijksinstituut voor Volksgezondheid en Milieu, 2011).
[7] For example, H. Bergmans, J. van der Horst, L. Janssen, E. Pruyt, V. Veldheer, D. Wijnmalen, M. Bokkerink, P. van Erve, and J. van de Leur, *Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands* (The Hague, Netherlands: Landelijk Operationeel Coördinatiecentrum, 2009); Anita Friend, *The UK National Risk Assessment* (Swindon: Global Uncertainties Annual Meeting, 2012); Charles Vlek, 'Response: What Can National Risk Assessors Learn from Decision Theorists and Psychologists?', *Risk Analysis*, vol. 33, no. 8 (2013), pp. 1389-93; M. G. Mennen and M. C. van

commentary on the broad structure of this process (Figure 1),[8] which translates essentially to the well-known steps in an integrated risk management or risk governance cycle.[9]

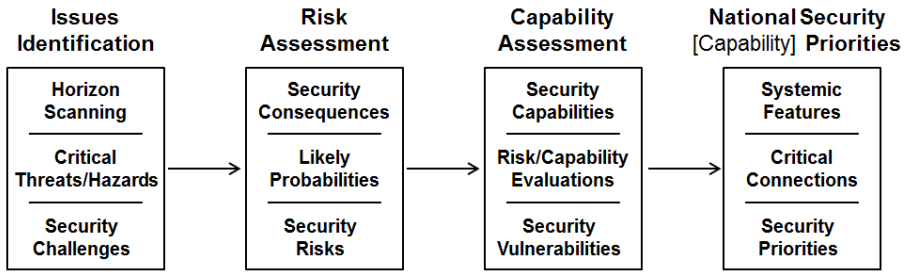

Figure 1: National security risk methodology

Source: Adapted from Alan Dupont and William J. Reckmeyer, 'Australia's National Security Priorities: Addressing Strategic Risk in a Globalised World', *Australian Journal of International Affairs*, vol. 66, no. 1 (2012), pp. 34-51.

However, the step from risk assessment to national security capability priorities is not well bridged and, in practice, relies on face-to-face discussion between experts and stakeholders without a tailored, designed process to guide those deliberations. The Dutch take this approach:

> Based on the risk assessment of all the scenarios analysed, an investigation is conducted to find out which capacities [capabilities] are already available and which of these could contribute to a reduction of the impact or the likelihood … The capability analysis takes place in a working group that includes all relevant experts and interests…[10]

Their process is typical in its use of risk-scoring, exemplar scenarios and expert panels.[11] An exemplar scenario is intended to represent a class of 'what ifs' about the future, for example, a chemical attack in a city's subway transport system. Expert panels generate risk scores by assessing the likelihood of each scenario and its impact on objectives. The same panels may then discuss capability requirements for addressing high-scoring risks.

Tuyll, 'Dealing with Future Risks in the Netherlands: The National Security Strategy and the National Risk Assessment', *Journal of Risk Research*, in press (2014).

[8] Alan Dupont and William J. Reckmeyer, 'Australia's National Security Priorities: Addressing Strategic Risk in a Globalised World', *Australian Journal of International Affairs*, vol. 66, no. 1 (2012), pp. 34-51.

[9] Ortwin Renn, *Risk Governance: Toward and Integrative Approach* (Geneva, Switzerland: International Risk Governance Council, 2005).

[10] Bergmans et al., *Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands*, p. 11.

[11] Mennen and van Tuyll, 'Dealing with Future Risks in the Netherlands'.

This largely common approach, is potentially deficient in a number of important respects:

- The validity of decisions based on the kind of risk-scoring seen in national assessments, using a risk assessment matrix,[12] a probability-impact grid,[13] or a likelihood-impact diagram,[14] is now much disputed and largely discredited.[15] The key issue here is a failure to account for the many uncertainties within the assessments.

- There is often a mismatch in level of detail between the risk assessment process and capability analysis, despite some recognition of the need to match levels of detail: "the incident scenario must be so specific that it is possible to deduce from it which capabilities will have to be brought to bear in that scenario".[16] The methodology must support traceability between capabilities and their risk-reducing effects.

- It is generally possible to treat a risk in several different ways, for example, by deterring, preventing, or disrupting an attack, or by protecting its potential targets from harm. Alternative approaches usually reflect differing security philosophies, e.g., a political preference for prevention. However, the risk-reduction effectiveness of available alternatives, and hence the ability to compare their benefit-cost is not, methodologically or practically, well understood or supported. It is commonly beyond the cognitive reach of experts to make comparative evaluations in the absence of a systematic method to guide their thinking.

- A capability is generally ascribed higher value, and hence higher priority, if it contributes to risk reduction in several scenarios, particularly if there are many such scenarios. For example, if the process identifies four cyber and two terrorist scenarios, then cyber-related capabilities may gain prominence (and priority) because they

[12] National Emergency Management Committee, *National Emergency Risk Assessment Guidelines* (Hobart: Tasmanian State Emergency Service, 2010).
[13] International Standards Organisation, *ISO/IEC 31010:2009: Risk Management: Risk Assessment Techniques* (Geneva: IEC, 2009), p. 82.
[14] World Economic Forum, *Global Risks 2013—Eighth Edition* (Cologny, Geneva Forum: World Economic Forum, 2013).
[15] Charles Vlek, 'How Solid Is the Dutch (and the British) National Risk Assessment? Overview and Decision-Theoretic Evaluation', *Risk Analysis*, vol. 33, no. 6 (2013), pp. 948-71; Louis A. Cox, Jr, 'What's Wrong with Risk Matrices?', *Risk Analysis*, vol. 28, no. 2 (2008), pp. 497-512; Douglas W. Hubbard, 'Worse Than Useless: The Most Popular Risk Assessment Method and Why It Doesn't Work', *The Failure of Risk Management: Why It's Broken and How To Fix It* (Hoboken, NJ: John Wiley & Sons, 2009); C. Chapman and S. Ward, 'Uncertainty, Risk and Opportunity', *How to Manage Project Opportunity and Risk: Why Uncertainty Management can be a Much Better Approach than Risk Management* (Hoboken, NJ: Wiley, 2011), pp. 43-71.
[16] Bergmans et al., *Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands*, p. 18.

appear more often in the analysis. While there is clearly additional value in capabilities that contribute broadly, it is important that the balance of exemplar scenarios appropriately reflect their relative weights in future possibilities, in order to avoid a potentially unwarranted bias of priorities.

- Often the role of exemplar scenarios is misunderstood, leading to an inability to create an appropriate balance of scenarios across the spectrum of threats, as discussed in the last point. Exemplar scenarios represent mutually exclusive portions of the future containing many possible pathways to impact. Typical resource limitations in the assessment process mean that each and every possible configuration of events leading to impact cannot be considered as a separate scenario. For practical purposes, exemplar scenarios should therefore be seen as classes of pathways. The danger inherent in such compression is that experts may assess them literally rather than as broad expressions of future possibilities.

It is known that judgments of experts and stakeholders relating to capabilities and priorities are strongly influenced by the particular method chosen for risk reduction assessment.[17] It is therefore very important to report the practice of assessment leading to capability prioritisation to enable constructive critique and improvement.

This article reports a method for identifying which of a nation's (existing or proposed) capabilities provide disproportionate value (in risk reduction terms) in the treatment of a spectrum of national security risks. Such capabilities perform critical functions in the national security architecture, which means that deficiencies or vulnerabilities associated with their roles are the logical targets for investment of limited resources. The method is founded on the risk standards,[18] but is intended to address the methodological deficiencies noted above.

The approach utilises a construct termed a risk pathway, which is a more detailed version of the commonly known 'bow-tie' diagram,[19] and is a more pragmatic form of engineering approaches like coupled fault trees and event trees.[20] Risk pathways are constructed to a level of detail that supports

[17] Kirsti R. Vastveit, *The Use of National Risk Assessments in the Netherlands and the UK* (Stavenger: University of Stavanger, 2011).
[18] Standards Australia and Standards New Zealand, *AS/NZS 4360:2004 Risk Management* (Sydney: Standards Australia and Standards New Zealand, 2004); International Standards Organisation, *ISO/IEC 31010:2009: Risk Management: Risk Assessment Techniques*.
[19] Julian Talbot and Miles Jakeman, *Security Risk Management Body of Knowledge* (Hoboken, NJ: Wiley, 2009).
[20] B. John Garrick, *Quantifying and Controlling Catastrophic Risks* (San Diego, CA: Academic Press, 2008); Dan S. Nielsen, *The Cause/Consequence Diagram Method as a Basis for Quantitative Accident Analysis* (Roskilde, Denmark: Danish Atomic Energy Commission, 1971);

assessment of the roles of capability, although not as individual contributions. Work elsewhere, associated with the concept of security-in-depth (SiD),[21] has shown that the only way to manage the complex inter-dependencies of capabilities and assess their risk reduction contributions, requires that they be considered in 'packages'. High-level concepts familiar in the national security lexicon such as prevent, prepare, respond and recover,[22] are related to, but not quite correct as choices for these packages, as we discuss in the next section.

Following a brief overview of the security-in-depth framework, 'Risk Assessment Using Risk Pathways' illustrates the construction of example risk pathways that are appropriately matched to the needs of capability planning. 'Risk Evaluation' highlights inadequacies of the risk matrix for determining risk treatments and capability needs, while 'Risk Treatment' discusses how this is much more effectively achieved. From the identification of required capabilities 'Identifying Capability Priorities' sets out the principles by which particular capabilities that are critical to risk reduction may be identified. The discussion then addresses the issues associated with aggregating capability priorities across risk pathways in order to gain a sense of strategic priorities. Finally, the article concludes with the advantages of the advocated approach over current practice.

Brief Overview of 'Security-in-Depth'

The security-in-depth (SiD) framework[23] is based on a hierarchy from ***security controls*** (the physical, technical, procedural elements of capability) that perform or contribute to ***security functions*** (higher-level constructs or 'security verbs' that include detection, alert, response, delay, neutralise, etc.), that, in appropriate combinations, constitute ***security layers.*** A typical security layer includes detection, alert and response functions because detection capabilities in the absence of a response, or response/neutralisation systems without a cue to act, are impotent in risk management terms. Security layers, as integrated sets of functions, are the smallest meaningful aggregation of capabilities that can stop harmful events or diminish their consequences.

Figure 2 shows a bow-tie diagram that conceptualises all possible pathways from threats to consequences. Superimposed onto the bow-tie are the

International Standards Organisation, *ISO/IEC 31010:2009: Risk Management: Risk Assessment Techniques*.

[21] Rick Nunes-Vaz, Steven Lord, and Jolanta Ciuk, 'A More Rigorous Framework for Security-in-Depth', *Journal of Applied Security Research*, vol. 6, no. 3 (2011), pp. 372-93.

[22] Attorney-General's Department, *Guide to Australia's National Security Capability*, p. 13.

[23] Nunes-Vaz, et al., 'A More Rigorous Framework for Security-in-Depth'.

seven layers of the strategic SiD framework.[24] Consequences (on the right side of Figure 2) are represented in two ways. Immediate impacts (or effects) are measured in terms such as lives lost, dollars incurred, disruptions to or losses of essential services, etc. However, depending on the resilience of physical, economic, infrastructural or social systems, these effects may or may not escalate into impacts of national security significance. For example, soon after the London bombings of 2005 the transport network was still operational through most stations (infrastructure resilience), and London commuters were still willing to use public transport (social resilience) in the face of remaining uncertainties.[25] Without such resilience, national impacts would have been far greater.

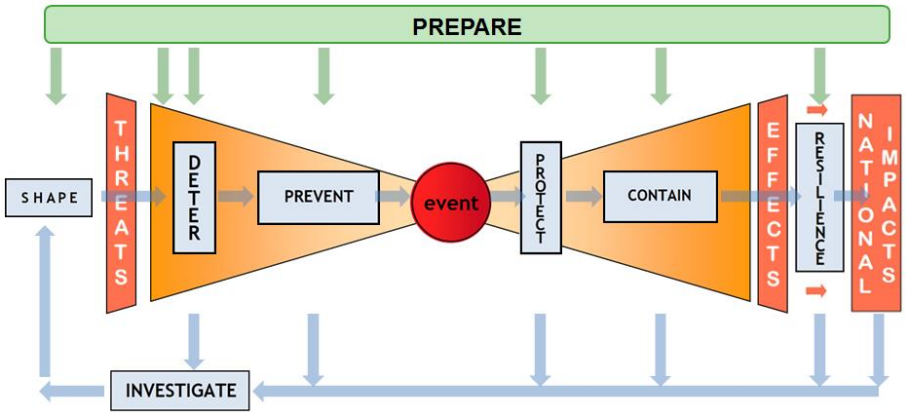

Figure 2: The Security-in-depth framework

The seven strategic layers of the security-in-depth framework (in blue), acting to reduce the probability of threat-initiated events and their potential to generate harm. The layers are deliberately orientated horizontally or vertically. Vertical alignment indicates a passive layer that requires pre-positioned capability. Horizontal alignment indicates an active layer with potentially many moving parts. Enabling capability and arrangements are represented within the construct called 'prepare'. All elements are described in the text.

Each security layer should be seen as an integrated set of functions, performed by many inter-dependent controls or capabilities, and individual capabilities can contribute to functions in more than one layer. The layers are aligned in sequence, that is, if 'shaping' does not resolve the threat, then

[24] This is the strategic version of the security-in-depth (SiD) framework, extended by three layers (shape, resilience and investigate) when compared with the version published in ibid.
[25] House of Commons, *Report of the Official Account of the Bombings in London Terrorist Attacks on 7 July 2005. HC 1087* (London: The Stationery Office, 2006); Norman Vasu, *Social Resilience in Singapore: Reflections from the London Bombings* (Singapore: Select Books, 2007); John Drury, Chris Cocking, and Steve Reicher, 'The Nature of Collective Resilience: Survivor Reactions to the 2005 London Bombings', *International Journal of Mass Emergencies and Disasters*, vol. 27, no. 1 (2009), pp. 66-95.

it may be 'deterred'. If not 'deterred' then the attack may be 'prevented', and so on. If the first six layers fail, the 'investigations' layer may help identify perpetrators or their associates in order to reduce risks associated with future events.

This layered construct is valuable for its completeness, that is, for illustrating the full set of opportunities for potential intervention and treatment in sequential stages from threat emergence to national impact rather than, for example, focusing on one aspect such as prevention.

A further dimension of the SiD construct involves a concept called 'prepare' (in Figure 2). Preparation manages the security risk that arises from internal failures of the security enterprise itself, rather than its failure to manage external threats (or hazards). Such failures may arise from poor organisational structures and arrangements, a failure to perform or deliver a role through poor resourcing, unreliable systems, etc., or potentially through the malicious actions of insiders.

Preparation in the SiD framework represents everything within and associated with the enterprise that must align in order for security to perform effectively. It is sub-divided into 'action', 'management' and 'policy' levels (note the distinction from 'layers') and is addressed in more detail elsewhere.[26] The concept represented by 'prepare' should be considered an enabler rather than a layer because, even if it performs perfectly, it does not reduce security risk (the criterion used to define security layers). If it performs less than perfectly it has a negative effect on the enterprise's ability to reduce security risk.

Risk Assessment Using Risk Pathways

For comparison with the stages of Risk Assessment, Risk Evaluation and Risk Treatment in the national and international standard the following three sections are titled to match.[27]

STRATEGIC OBJECTIVES

The Standard defines risk in terms of impact on objectives. National security objectives are defined or articulated within a nation's suite of strategic documentation,[28] and are commonly couched in terms of limiting

[26] From Rick Nunes-Vaz and Steven Lord, 'Designing Physical Security for Complex Infrastructures', *Journal of Critical Infrastructure*, in press (2014), following D. M. Murphy and M. E. Pate-Cornell, 'The SAM Framework: Modeling the Effects of Management Factors on Human Behaviour in Risk Analysis', *Risk Analysis*, vol. 16, no. 4 (1996), pp. 501-15.
[27] Standards Australia and Standards New Zealand, *AS/NZS ISO31000:2009 Risk Management: Principles and Guidelines* (Geneva, Switzerland: IEC, 2009).
[28] Australian Government, *Strong & Secure: A Strategy for Australia's National Security*, (Canberra: Department of the Prime Minister & Cabinet, 2013); Canadian Government, *Canada's National Security Policy*; UK Government, *The National Security Strategy of the*

- physical harm
- social/psychological harm
- economic harm
- reputational harm

to the nation or its citizens, and

- violations of sovereignty or territorial integrity.

Strategic risk assessment is then an examination and evaluation of threats to those objectives.

SOURCES OF RISK

Horizon scanning, scenario analysis and other techniques are typically used to anticipate, identify and assess all potential sources of risk (i.e., threats). National security strategies commonly identify these risk sources to include:

- State-based conflict
- espionage
- terrorism, and
- organised crime.

Depending on a nation's view of national security, they may also include natural hazards, such as:

- infectious human, animal or plant disease
- flood, fire, earthquake etc., and
- industrial accident.

ARTICULATING RISKS IN TERMS OF PATHWAYS

To reveal the contributions of national security (NS) capabilities to the reduction of risk to objectives requires the articulation of national security impacts from each risk source in the form of a risk pathway.[29] A bow-tie

United Kingdom; US Government, *The National Strategy for Homeland Security*; Kevin Rudd, *Speech by the Prime Minister to the Parliament: The First National Security Statement* (Canberra: Department of the Prime Minister & Cabinet, 2008).

[29] 'National security impacts' is shorthand for impacts to national security objectives.

diagram is known to be insufficiently detailed to support this.[30] Figure 3 shows a generic risk pathway,[31] associated with a malicious threat such as crime or terrorism. Once the actors' intent is formed, they must acquire capability, formulate a plan and conduct an act. Their actions are, in general, intended to benefit a cause (shown in the lower 'return loop'). The act may itself be of national security significance or it may trigger a cascade of effects that generate impacts of national security significance.

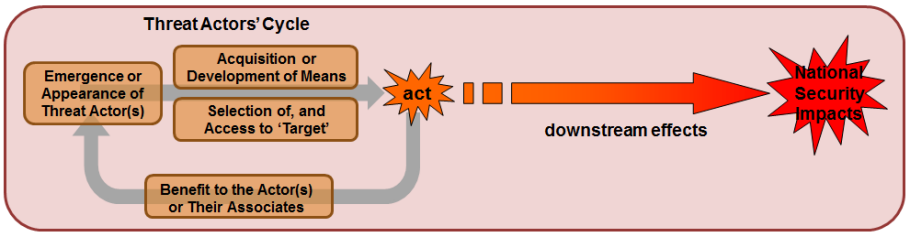

Figure 3: National Security Risk Event

A generic representation of a national security risk event as a pathway from the emergence of threat actors to the generation of national security impacts.

REPRESENTING THE SPECTRUM OF THREATS: COMPLETENESS

Flexibility and adaptability are present and valued in capabilities that play broad emergency management roles. Other capabilities, however, though much less flexible are equally important in other scenarios, such as sensors for detecting specific harmful chemical or biological agents. To understand the relative priorities of such diverse capabilities first requires a comprehensive set of risk pathways to represent the scope of potential problems.[32]

The challenge in developing such a set, however, lies in the difficulty of ensuring that it is comprehensive, yet not repetitive. As a primary objective of the whole process is to gain a sense of capability priorities, it is important not to over-represent some concerns (pathways) relative to others. To achieve this, the set of risk pathways should be developed by all relevant

[30] International Standards Organisation, *ISO/IEC 31010:2009: Risk Management: Risk Assessment Techniques*, p. 65.
[31] We use the words 'pathway' and 'scenario' interchangeably from here, understanding that these scenarios are of the specific type, specifying a risk source and how it leads to impacts.
[32] S. Myagmar, A. J. Lee, and W. Yurcik, 'Threat Modeling as a Basis for Security Requirement', Symposium on Requirements Engineering for Information Security (SREIS 2005), Paris, France, 2005.

stakeholder agencies with three over-riding guiding principles as noted in other scenario studies:[33]

- Each risk pathway must be a complete sequence from the emergence or appearance of the threat or hazard through to its generation of harm.
- Each risk pathway must be mutually exclusive.
- Each scenario should translate into a distinct pathway inasmuch as each differs in a meaningful way from others, with regard to capability and the scope of the national assessment. It is possible to generate many attack pathway variations, even though each would stress treatment capability in largely the same manner. Judgment is needed to maximise coverage while minimising redundancy with respect to capability-needs assessment. Subsequent assessment of any particular pathway requires consideration of all the variants 'compressed' within its representation, rather than taking a literal view.

LEVEL OF DETAIL

The level of detail in Figure 3 is, in practice, too coarse to be useful. The risk pathways are expanded in relation to each source of risk and the expansion continued to a level of detail that matches the understanding or articulation of risk treatment (national security) capabilities. In practice there will be iteration between pathway detail and the matching capability discussion, as we address in 'Risk Treatment' below .

An example pathway representing an unspecified terrorist attack is shown at the foot of Figure 4. Each step in the pathway represents an opportunity for intervention and the application of security capability. Two elements of the pathway, that is, 'motivated actors' and 'acquire means' have been expanded in the upper part of Figure 4. There are two implications of expansion in this manner. The first is that expansion reveals additional opportunities to intervene and manage, in these cases, the probability of the pathway progressing to completion. The additional detail is useful if there are capabilities that can be applied or developed to reduce these probabilities. The second implication is that some sub-pathways can be developed and re-used, in similar form, in a number of different pathways. We have found a modular approach to pathway construction useful in practice.

[33] Bergmans et al., *Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands*; R. Bradfield, G. Wright, G. Burt, G. Cairns, and K. van der Heijden, 'The Origins and Evolution of Scenario Techniques in Long Range Business Planning', *Futures*, vol. 37 (2005), pp. 795-812; M. Godet, *Creating Futures: Scenario Planning as a Strategic Management Tool* (Paris: Economica, 2006); Kees van der Heijden, *Scenarios: The Art of Strategic Conversation* (Hoboken, NJ: John Wiley and Sons, 2005).

Specifically, we have found two types of modular sequence useful. The radicalisation and weapon development modules are examples of what we call precursor sequences. They are invoked whenever a complex process remains implicit within an element of the risk pathway.

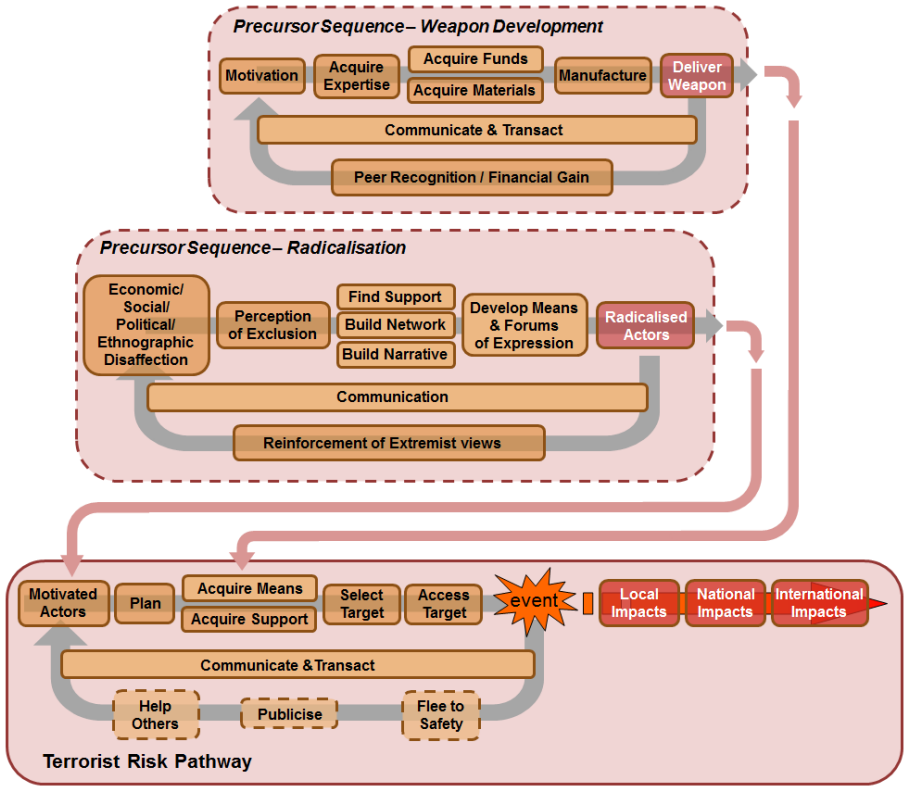

Figure 4: Terrorist Attack Pathway

A plausible representation of a terrorist attack pathway (lower part of the figure), with two precursor sequence modules (i.e., weapon development and radicalisation) essentially expanding the target elements of the main terrorist pathway. Only the terrorist pathway is a risk pathway because it includes a defined event and its consequences. The dashed elements in the terrorist pathway are intended to represent activities that may or may not occur.

The other type of pathway module is a 'disabling sequence'; an example of which occurs in Figure 5. The disabling sequence allows us to represent compromise, disruption or failure of the security machinery itself (represented in blue without detail in Figure 5). Compromise may occur as the result of deliberate or malicious interference (or deliberate inaction) arising, for example, from sabotage or corruption by organised crime or 'insider' agents, as shown. It can also arise from a failure in preparation (as

we discuss below in the section 'Preparation') when, for example, a critical detector fails due to inadequate maintenance, and the need for a replacement was never considered. Even though disabling sequences represent 'attacks' on the machinery of security, their expression as pathways reveals the nature of opportunities to intervene to preclude or limit the potential for compromise.

A third type of pathway module involves follow-on or indirect impacts from events (with two such modules illustrated in Figure 5). Events from several sources of risk, such as state-conflict, state fragility, terrorism or pandemic may lead to follow-on impacts from mass migration or civil unrest, for example. Again, the expression of follow-on effects as pathways reveals the opportunities to contain, protect against, or be resilient to their evolution into national security impacts.

Risk Evaluation

Common practice, at this stage, would see subjective risk evaluation of each pathway,[34] in which experts assess the likelihood (roughly, the chance that each scenario will occur, or how frequently it is expected to occur in a future time period), and the band of consequences that most closely represents the risk's impact. By this process each scenario is allocated into a cell of a matrix representing risk magnitude.[35]

However, it is inappropriate to assign priority to a capability based on the magnitude of risk of a pathway that invokes it, that is, a high risk pathway implying high priority capabilities.[36] Firstly, while there may be a strong imperative to mobilise, innovate and develop resources to tackle the, possibly existential, risks in the high likelihood, high consequence corner of the matrix, greater risk reduction for the same cost is generally the guiding principle in government decision-making.[37] It is the reduction in risk from the use of particular treatments, not whether the treatments address a high risk, which is most relevant to prioritising capabilities.

---

[34] Standards Australia and Standards New Zealand, *AS/NZS ISO31000:2009 Risk Management: Principles and Guidelines*.

[35] Betty E. Biringer, Rudolph V. Matalucci, and Sharon L. O'Connor, *Security Risk Assessment and Management: A Professional Practice Guide for Protecting Buildings and Infrastructures* (Hoboken, NJ: John Wiley, 2007); Talbot and Jakeman, *Security Risk Management Body of Knowledge*; Cabinet Office, *National Risk Register of Civil Emergencies: 2012 Edition*; Stephane Jacobzone, 'Country Risk Assessment and Management', 4 October 2012, <http://www.irgc.org/wp-content/uploads/2012/10/4.-Stephane-Jacobzone_CRA_IRGC-Beijing-2013.pdf> [Accessed 15 January 2014]; Julian Talbot, 'What's Right with Risk Matrices?', <http://www.jakeman.com.au/media/whats-right-with-risk-matrices> [Accessed 14 January 2014]; Friend, *The UK National Risk Assessment*.

[36] Andy Garlick, *Estimating Risk: A Management Approach* (Aldershot: Gower Publishing, 2007).

[37] Australian Government, Office of Best Practice Regulation, *Best Practice Guidance Note: Decision Rules in Regulatory Cost-Benefit Analysis* (Canberra: Department of Finance and Deregulation, 2009).

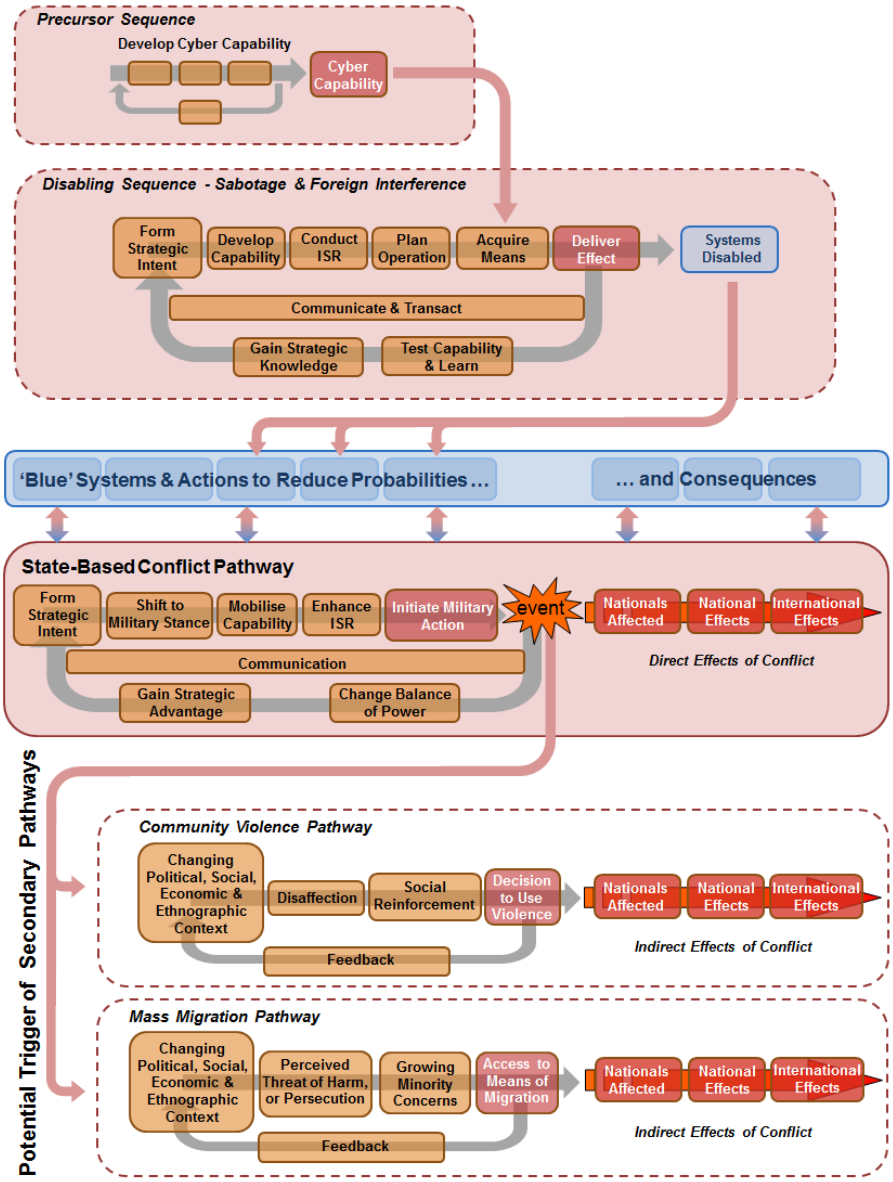

Figure 5: State-based Conflict Pathway

A more detailed example of pathways representing adversary-initiated state-based conflict (centre) leading to national security consequences. Friendly, defensive capabilities are represented without detail in blue. The adversary has employed two additional (modular) sequences at top, that is, a cyber capability development precursor sequence which supports another sequence intended to disable defensive systems. Similar modularity is seen in the lower part of the figure in the form of two follow-on pathways (community violence and mass

migration) triggered as indirect effects of the conflict. Many other indirect effects could be explored. Every step in a sequence provides opportunities for countermeasures and hence the identification of national security capability needs.

In fact, it is easy to manipulate, whether intentionally or inadvertently, the magnitude of risk that is attached to a scenario when using the risk matrix approach. This can be done by changing scenario detail. More specific scenarios correspond to a smaller proportion of the future, which means lower likelihood and therefore lower risk. A high risk pathway in the matrix approach may be broken down into several lower probability or lower consequence sub-pathways. This is a common tactic when risk management is focused on compliance. One can always make a project comply with risk tolerance limits by increasing the specification of relevant scenarios.[38] This is just one aspect of the ambiguity risk matrices generate because they provide no information on the issue of risk aggregation.[39] Appropriate aggregation would show that the low risk sub-pathways add up to the high risk parent pathway, so the assessment should be independent of scenario specification. As scenario specification does have a direct bearing on the risk assessment process, translation to capability priorities requires care to manage risk magnitude and risk aggregation appropriately. As already noted, priority should relate to risk reduction rather than risk magnitude, as discussed in the next section. The aggregation problem is discussed in the section 'Identifying Capability Priorities'.

A further point, although still related to aggregation, is about inter-dependency between national security threats.[40] Capabilities usually treat sources of risk, and those sources may appear in several risk pathways, for example, anti-virus software treating cyber threats that occur in both 'terror' and 'crime' pathways. To assess the value of such capabilities we must be able to examine all relevant pathways and aggregate (in some sense) their contributions to the treatments that reduce risk. The inter-relationship between threats means that the capabilities required to treat a particular risk (represented by one marker in a risk matrix) should not be considered in isolation from their role elsewhere (associated with other markers in the matrix).

We therefore advocate that evaluating the risk magnitude of pathways (scenarios) is not useful at this stage. As distinct from current practice, we do not risk-score pathways until they have been developed to the resolution required to judge the needs and values of risk treatments.

[38] Health and Safety Executive, *Good Practice and Pitfalls in Risk Assessment. Research Report No. 151* (Sudbury: HSE, 2003).
[39] Louis A. Cox, Jr, Djangir Babayev, and William Huber, 'Some Limitations on Qualitative Risk Rating Systems', *Risk Analysis*, vol. 25, no. 3 (2005), pp. 651-62; Cox, 'What's Wrong with Risk Matrices?'.
[40] Dupont and Reckmeyer, 'Australia's National Security Priorities'.

Risk Treatment

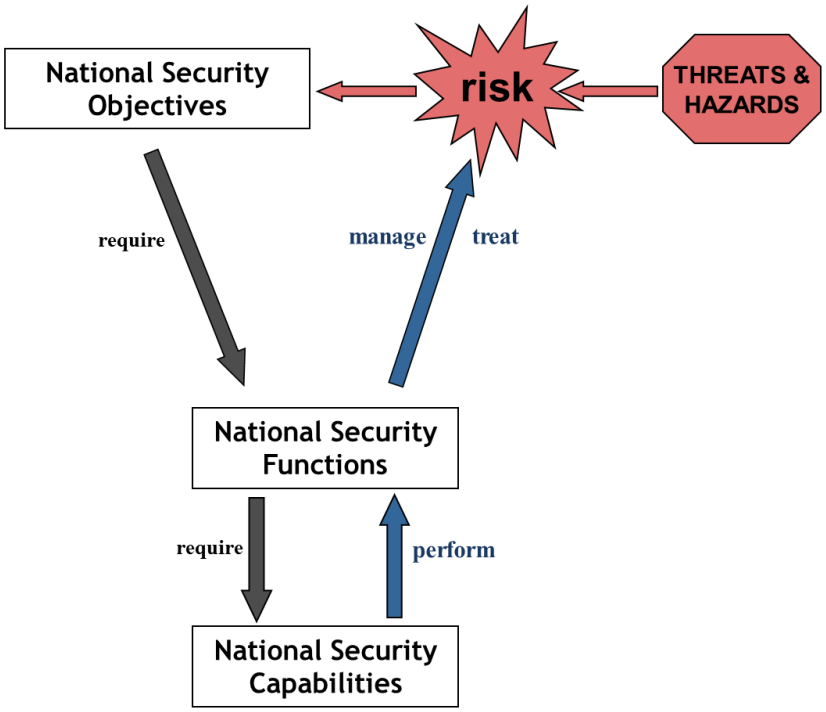

Figure 6: Risk Treatment

Threats and hazards represent sources of risk with respect to strategic security objectives. Treatment of risk requires the performance of functions or tasks which require the application of capabilities.

Risk treatment (Figure 6) is achieved through the effective application of national security capabilities (e.g., Customs' maritime patrols), performing required functions (e.g., law enforcement).[41] A sense of priorities comes from understanding the relative contributions to risk reduction that can be achieved, and this is assessed using the SiD framework.

ALLOCATING CAPABILITIES TO RISK TREATMENT

Figure 7 shows an expansion of the generic pathway relating to terrorism at the foot of Figure 4, truncated where the terror act occurs. A notional border has been added, distinguishing offshore from onshore elements of this particular pathway, and four regions are identified (international, border, national and local) representing different contexts for security intervention.

[41] Attorney-General's Department, *Guide to Australia's National Security Capability*.

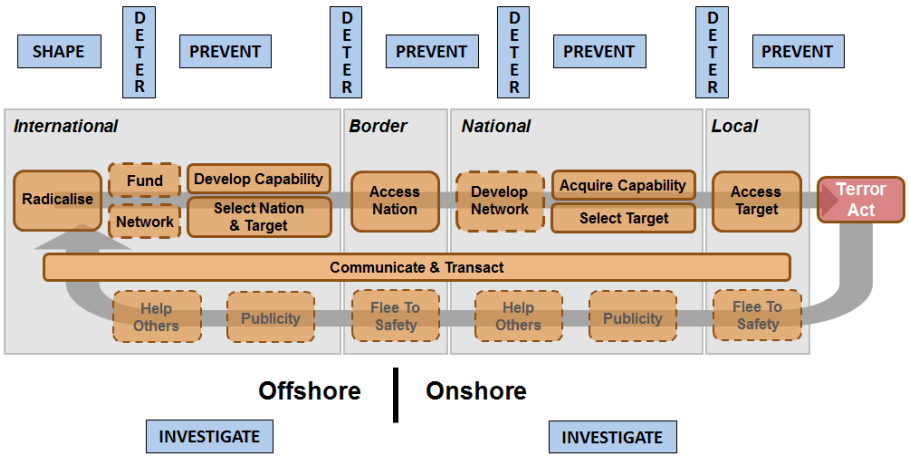

Figure 7: Cross-border Movement

A more detailed representation of the cross-border movement of terrorists and their capability, highlighting the way that context focuses the interpretation of relevant capability.

The figure shows the layers of security that might be applied to treat the risk. For example, the explicit pathway component marked 'radicalise' might be treated using capabilities that contribute to 'shaping' the relevant offshore communities. Multiple instances of security layers are often needed, so a hypothetical overseas terrorist may be deterred or prevented prior to their overseas departure (where intelligence sharing and cooperation are strong); at the border (immigration officers); within the national system (federal police); or by the local security associated with the target itself (gates, guards, etc.).

Figure 8 shows an example of the way that expansion of the pathway proceeds to support understanding of capability needs. The 'develop capability' element of Figure 7 requires the terrorists to acquire expertise, acquire materials and then manufacture the capability. The lower part of Figure 8 shows examples of capabilities that might prevent each of the steps. Prevention requires the successful performance of detect, alert and respond functions which, in turn, demand the successful operation of potentially many integrated capabilities, some examples of which are shown in the figure. By increasing the level of detail in the pathway, commensurate detail can be developed in the array of potential treatments, from which the implications for capability can be assessed.

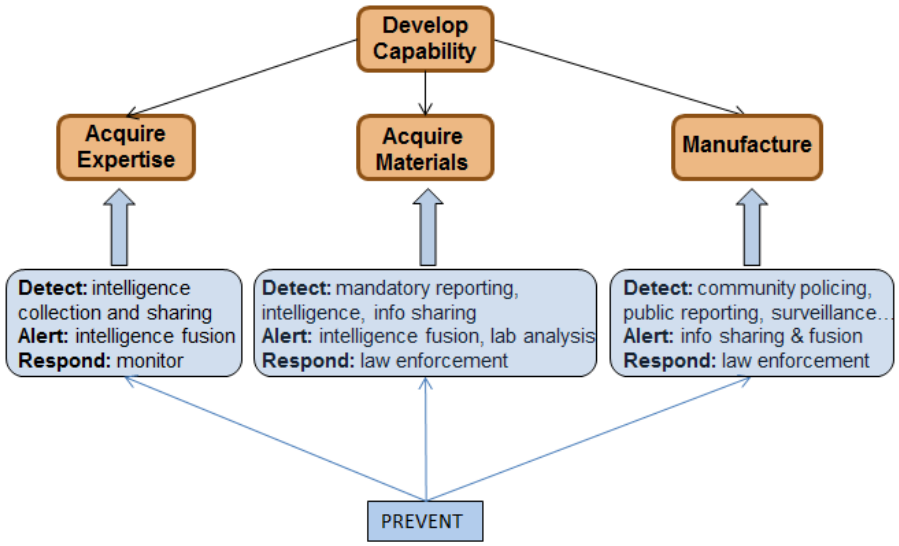

Figure 8: Developing Capability

An expansion of 'develop capability' from Figure 7, with example capabilities that might be used to treat the elements. Note that the prevent layer requires the performance of all three functions of detect, alert and respond and each, in turn, requires appropriate capabilities, only some of which are shown for illustration.

Other layers, beyond prevent, are then examined in similar manner. Expansion of pathways should ensure that the resolution of pathway elements matches the resolution of capabilities being considered. In this way, the expansion and discussion of risk pathways is intimately tied to the discussion of capability needs, and should not be separated as a sequential process.[42] The net result is a layering of capabilities along the pathway between the sources of risk and impacts.

Figure 9 shows a further illustration of the use of pathway sequences to identify capability needs. The disabling sequence illustrated in Figure 5 shows an adversary's use of cyber capabilities to compromise national defence systems involved in state-based conflict. The disabling sequence itself provides opportunities for treatment (countermeasures) as shown, in partially developed form, in Figure 9.

[42] Stephan De Spiegeleire, 'Ten Trends in Capability Planning for Defence and Security', *The RUSI Journal*, vol. 156, no. 5 (2011), pp. 20-8.

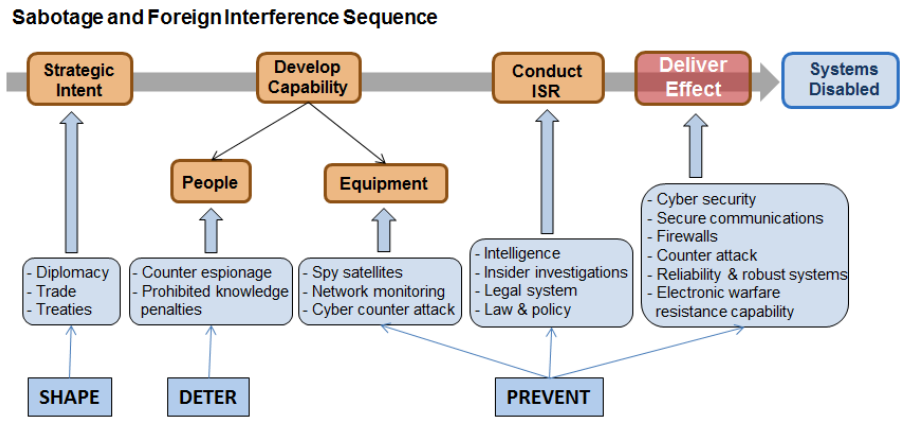

Figure 9: Cyber Countermeasures

Example countermeasures associated with shaping, deterring, and preventing sabotage or foreign interference by cyber means. These are countermeasures intended to reduce the probability and the potential impacts of adversary action.

LAYERS AND THEIR FUNCTIONS

Shape, prevent, contain and investigate layers (the horizontal layers in Figure 2 and Figure 7) all rely on the successful performance of variants of detect, alert, respond and impede functions. A successful investigate layer, for example, relies on the detection of clues (evidence), piecing enough parts of the puzzle together to warrant raising the alarm, and some interdiction capabilities.

In general, the passive layers (deter, protect and resilience) rely on single, context-specific functions. Deterrence largely derives from the perceived effectiveness of security (ignoring the contribution from the severity of penalties, if convicted),[43] which can be manipulated using real or purported capability. Protection is highly context-dependent, so protection from crime, bombs, fire, floods, disease, etc., all require very different and very specific capability sets. Suitable protections can be identified by asking "what are we protecting, and from what?"

Some aspects of resilience are passive, such as the social resilience of London commuters and their use of public transport after the 2005 bombings. This kind of social resilience is developed in the system prior to an event and derives from people's perceptions of risk, which is also subject

[43] Andrew R. Morral, Brian A. Jackson, Corporation Rand, and Security Rand Homeland, *Understanding the Role of Deterrence in Counterterrorism Security* (Santa Monica, CA: RAND, 2009); Paul K. Davis and Brian Michael Jenkins, *Deterrence and Influence in Counterterrorism* (Santa Monica, CA: RAND Corporation, 2002); Samuel J. Rascoff, 'Counterterrorism and the New Deterrence', *NYU Law Review*, vol. 89, no. 3 (2014).

to enhancement or manipulation, through communication. Active components of resilience are based on detect, alert and respond functions. For example, resilience in the London transport system relied on detection of non-functioning components and re-routing to restore operations to the highest possible level.

PREPARATION

Primary security capability relies on the availability and quality of enablers such as training, communications, information systems, logistics, etc. These enablers will often be as important to the effective performance of security as the security systems themselves. Preparation also involves alignment between management and policy and the needs of security risk management. A mismatch, for example, between a role and the authority to conduct that role, or its foundation in law, may disable or limit the effectiveness of security. Thus failure of enabling systems, collectively termed 'preparation', can substantially compromise security. Preparation is closely related to the notion of enterprise or intrinsic risk.

Figure 10 shows a sequence of elements for which inadequacy or failure of any one may lead to compromised risk treatment capability. The items shown are illustrative only, and are not intended to be exhaustive. This kind of breakdown and analysis, which is related to fault tree analysis, can be used to understand the context and implications of failures of enterprise risk management.

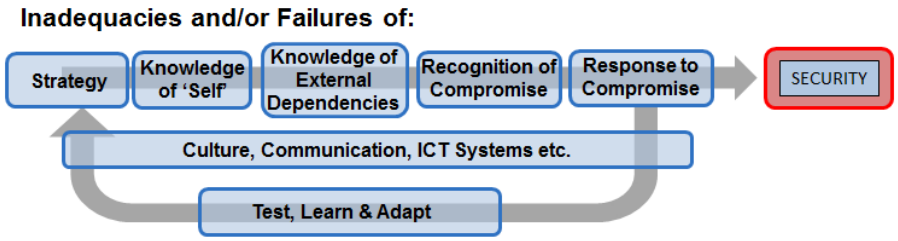

Figure 10: Enterprise Risk

A non-exhaustive sequence representing elements associated with intrinsic or enterprise risk. The failure of one or more elements leads to compromise of security.

In the feedback arrow in Figure 10 we see another role of 'prepare', which is to promote and enable self-awareness, contextual sensitivity, and the ability and propensity to monitor and assimilate lessons from both internal and external events, in order to identify the drivers for development.

Identifying Capability Priorities

INVESTMENT WITHIN LAYERS

The processes in the previous section are intended to lead, through cross-departmental and stakeholder consultation and discussion, to a determination of treatment options, in the form of a list of capabilities (and their enablers) required to manage the risks of all relevant pathways. The purpose of this section is to guide, using security-in-depth, the identification of critical capabilities from what may be a long capability list. A critical capability is one that a) when absent or damaged 'substantially' impairs the overall system's performance, and b) should be considered a target for investment because each increment of enhanced performance has high payoff in overall risk reduction effect. Performance should be judged in the context of the whole layer.

The security-in-depth framework works on the basis of risk reduction contribution. In SiD, within any single (multi-function) layer investment should be focused on the security function that performs least well.[44]

To make these assessments it is not always necessary to know precise performance figures for the functions. Consider the case of preventing the cross-border passage of contraband through an airport or seaport. Ports are designed to ensure that there is a high probability of both raising an alert and successfully interdicting the threat when a true-positive detection is made. Successfully preventing the passage of contraband therefore often relies most heavily on detection of the threat, and the prevent layer is therefore compromised inasmuch as detection probability remains comparatively low. If these assumptions are correct, the prevent layer's effectiveness would be improved by investing in detection.[45] Domain experts are often able to assess which function, in any given layer, is comparatively weak, and they or others can usually identify how to best enhance its performance within a defined budget.

Further examination shows that there are two ways to lift the performance of the detection function, and hence two candidate strategies for investment.[46] The first is to improve the performance of detection systems *in situ*, perhaps by increasing the percentage of goods that are screened or by investing in more advanced screening technologies to reduce the number of false negatives and false positives. Alternatively, detection might be improved by enhancing the probability that cueing information will be received prior to the contraband's arrival at the border. One way to do this is to raise the quality

[44] Nunes-Vaz et al., 'A More Rigorous Framework for Security-in-Depth'.
[45] Assuming that each dollar spent generates a similar incremental improvement in each function.
[46] Assuming that performance is not currently limited through compromised enablers like training.

of intelligence feeds into border operations, which might be achieved by enhancing information sharing arrangements with other nations.

Given the assumptions stated or implied in this example, the security objective of contraband interdiction implies that enhancement of detection capabilities is critical. Decisions on the best way to achieve that enhancement should then be resolved using cost-benefit principles.

INVESTMENT ACROSS LAYERS

Given that it is possible to identify the most cost-effective ways to enhance a security layer with respect to a given risk pathway, the next question is, which layer(s) deserve(s) greater investment. It is known that investment should be directed, counter-intuitively, to the layer which is already the best performer.[47] The layers are sequential, independent risk reduction systems which means that, theoretically, effective security only requires one layer to be successful. If prevention is successful then protection, containment and resilience are, in that instance, not required. Requiring only one successful layer means that investment should be directed to the layer that is most likely to achieve the overall security objective, that is, to the best performing layer. This conclusion, however, carries a number of caveats.

The first caveat is that layers perform differently with respect to different threats and scenarios. For example, choosing to protect against violent extremism requires that all potential targets be protected (because an intelligent adversary can learn which remain relatively unprotected).[48] This implies that a strategy focusing on protection will either be very costly or relatively weak. Contrast this with a bio-threat, for which protection (e.g., vaccination) may be much the most effective strategic approach.

The second caveat notes that a perfect layer is often difficult to achieve and investment should be sensitive to the returns that can be achieved, particularly where they progressively diminish. For example, deterrence may perform quite well against terrorism but statistics indicate that some attackers will remain undeterred. Rather than trying to further enhance deterrence, which will climb in cost and remain ineffective against the most determined adversaries, it is more beneficial to invest in (an)other relatively effective layer(s).

For some individual risk pathways all layers may be compromised, to some extent, and it may be difficult to identify the 'best' target for enhancement. In this case, several layers may contribute to risk reduction, not necessarily equally but perhaps comparably. In some cases, it may be possible to understand trade-offs between layers (the value of focusing investment in

[47] Nunes-Vaz et al., 'A More Rigorous Framework for Security-in-Depth'.
[48] V. M. Bier, 'Choosing What to Protect', *Risk Analysis*, vol. 27, no. 3 (2007), pp. 607-20.

some layers rather than others) using robust quantitative analysis.[49] However, national assessment currently falls into the category of being so complex that even subjective opinions about the sequential actions in risk pathways, and ontological uncertainty about modelling the risk pathway interactions, are likely to lead to inaccurate assessment. Strategic decision-makers may also be less than comfortable with such a step. Since it can be difficult to assess these trade-offs, we consider it more useful to assess all seven layers and ask which functions, in each layer, should be considered the primary targets for investment. The decision to focus investment into a particular layer might be made for reasons other than risk, for example, for political, social or economic reasons, such as the choice to protect particular iconic targets against the potential effects of terrorism. Freed from a requirement to prioritise between layers, each layer should be examined to identify its weakness in order to determine critical capabilities (and their enablers) on a per layer, per risk pathway basis. Illustrative results from such an analysis are shown in Figure 11.

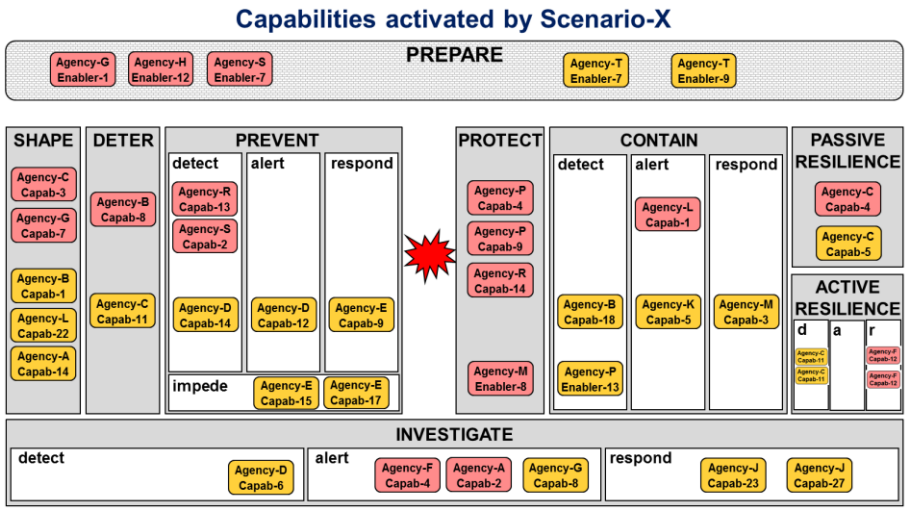

Figure 11: Risk Scenario

The results of analysis of (hypothetical) scenario-X, in terms of the capabilities in each layer required to manage its risk. Critical capabilities are shown in red, noting that they lie inside the functions that were identified as relatively weak in their layer context. A red capability may represent weakness in an existing system, or it may represent a missing capability that the analysis has exposed. Note that enablers are also included in the diagram (principally, although not exclusively, inside 'prepare').

[49] Steven Lord and Rick Nunes-Vaz, 'Designing and Evaluating Layered Security', *International Journal of Risk Assessment and Management*, vol. 17, no. 1 (2013), pp. 19-45.

In general, the analysis will identify 'packages' rather than individual capabilities that are disproportionately important to a layer's effectiveness. Figure 11 shows such capabilities in the seven security layers, and the enterprise enablers associated with 'prepare', from an analysis linked to hypothetical 'Scenario-X'. Those critical capabilities might already exist but may be under-performing, or they may not yet exist. This kind of analysis, as an output of stakeholder discussions, becomes an input to decision-making.

DETERMINING STRATEGIC CAPABILITY PRIORITIES

The previous section outlined a process by which critical packages of capabilities are identified in each layer, for each particular risk pathway. Pathways are themselves components in a de-aggregated view of the whole strategic security landscape.

Attempting to aggregate findings by adding up, across all pathways, the number of times a particular package is assessed to be critical will, as noted in the section 'Risk Evaluation', lead to bias and sensitivity to the particulars of de-aggregation, that is, the choice and balance of pathways represented. A more justifiable approach involves aggregating a package's contribution to risk reduction across all pathways. The difference between the two approaches is illustrated through Tables 1 and 2.

In Table 1, each pathway or scenario is risk-scored and each particular package receives an aggregate score across all scenarios from the product of the scenario risk and whether the package was judged to be critical (scoring a one) or not (a zero). Given cost estimates for each package, a form of benefit-cost ratio (BCR) is then generated in the final column. However, as discussed above in the introduction and 'Risk Evaluation', this form of scoring attaches importance to risk magnitude and does not assess overall risk reduction contribution. It provides only a weighted frequency of criticality for each package.

Table 1: Notional weighted scoring of capability packages due to binary view of criticality (1 for critical in scenarios and 0 if not)

	Scenario 1	**Scenario 2**	**Scenario 3**	**Score**	**Cost ($m)**	**BCR**
Risk (Expected Impact)	4	2	7			
Capability Package A	1	0	1	11	4	2.75
Capability Package B	0	1	1	9	4	2.25
Capability Package C	1	1	0	6	3	2

A stronger basis for strategic investment choices[50] is based on risk reduction assessment and true cost-benefit techniques. In Table 2 stakeholders assess the risk reduction provided by a capability package for each scenario, which can be elicited directly, or by subtracting estimates of residual risk from an initial risk. The total risk reduction of each package is then achieved through summation, leading to a more appropriate benefit-cost ratio which, in this illustration, implies different investment priorities.

It is in the problem of strategic aggregation that we believe the method described here is most useful. By breaking the complex interaction of interventions and threats into pathways, layers and functions in the manner that leads, through discussion, to constructs like Figure 11, stakeholders are able to greatly improve their subjective estimates of probability and consequences reductions.

Table 2: Notional benefit-cost of capability packages using a risk reduction view of criticality

	Scenario 1	**Scenario 2**	**Scenario 3**	**Total Red.**	**Cost ($m)**	**BCR**
Expected Impact before	4	2	7			
Expected Impact after						
Capability Package A	2.5	2	4.5	4	4	1
Capability Package B	4	1	3	5	4	1.25
Capability Package C	1.5	1	6.5	4	3	1.33

Neither approach, however, will necessarily identify a capability package that has relatively small benefit in any particular scenario, but which aggregates to a high total risk reduction across all pathways. This flaw should be highlighted in decision-making discussions, and a separate check conducted in the aggregate analysis.

The benefit in the BCR in Table 2 is the expected reduction in impact using the single metric of discounted cost or, more accurately, de-utility measured by discounted cost, for impact.[51] Strategic agencies may wish to retain several benefit-cost indices, (economic cost, lives lost, reputation, etc.), in which case techniques of multi-criteria optimality or ordering (through Pareto fronts and Pareto domination) can be used.[52]

[50] National Commission of Audit, *Towards Responsible Government: The Report of the National Commission of Audit* (Canberra: Commonwealth of Australia, 2014).
[51] Attorney-General's Department, *Submission to the Productivity Commission Inquiry into Natural Disaster Funding Arrangments* (Canberra: Attorney-General's Department, Commonwealth of Australia, 2014), p. 6.
[52] Yacov Y. Haimes, *Risk Modelling, Assessment, and Management* (Chichester, UK: Wiley, 2004); J. Figueira, S. Greco, and M. Erghott, *Multiple Criteria Decision Analysis* (New York: Springer, 2005).

Uncertainty is a major issue in subjective estimates (of both benefit and cost) in the complex environment of national security. It is beyond the scope of this article, but there are existing statistical techniques that allow uncertainty in subjective opinion to be elicited and characterised, and to be retained in cost-benefit assessments. When dealing with uncertainty one should look at other possible future values apart from expected value: the industry standard in finance is to consider the worst 5 per cent of outcomes as well as the expected outcome.

As a final point, capability development and acquisition processes generally span several years or even decades, particularly in military capability acquisition. Therefore, discounting or inflating future benefit should consider indicators of trends. An obvious example here is the potential growth (in both frequency and severity) of cyber-attack scenarios. For this reason, it makes more sense to measure risk reduction and the ratio of risk reduction to cost for capability packages rather than simply risk assessing scenarios. A strategic threat may endure, but the performance of capabilities over time generally will not, and it is the latter which is relevant.

Summary

Despite significant and growing arguments in the literature about the flaws surrounding the use of risk (likelihood-consequence, probability impact) matrices in decision-making, national security agencies in western nations continue to use these devices presumably because of their relatively intuitive (but inappropriate) basis for prioritising capabilities and allocating resources according to risk magnitude. While it is reasonably understood and accepted that investment of resources should be governed by benefit-cost considerations, disproportionate allocation of resources to higher risks is often justified through (potentially flawed) assessment that identifies certain risks to be high, and because assessing risk reduction benefit is felt to be methodologically difficult. No nation has yet articulated a practical method for assessing the strategic risk reduction value of particular investments, or a means to compare alternative risk treatment strategies. The Dutch do note the importance of considering multiple factors, not just risk magnitude, but it is still common to see investment decision ratings as an overlay placed directly onto the risk matrix.[53]

Ultimately we believe that currant approaches have limited defensibility according to risk and governmental Standards. The approach in this article addresses these flaws by providing a means to assess and evaluate the risk reduction contributions of treatments and capabilities. We depart from established methods in three fundamental ways. Firstly, there is no need to define the likelihood-consequence bands (the specific cell in a risk matrix)

[53] Michel Rademaker, 'National Security Strategy of the Netherlands: An Innovative Approach', *Information & Security: An International Journal*, vol. 23, no. 1 (2008), pp. 51-61.

that a particular threat or hazard belongs to and give it a specific or implied score in isolation from consideration of relevant treatment capabilities. It is far more useful to articulate the path by which a source of risk (e.g., a terrorist) can cause harmful consequences, because it is the steps along the risk pathway that provide opportunities for intervention and the application of capability. Development of risk pathways, by the policy and intelligence communities, working alongside the capability owners and operators ensures that the fidelity of each step in the pathway is tailored precisely to the process of gap analysis and capability-needs assessment.

The second departure from orthodoxy centres around the unit or quantum by which capability values are assessed. Through inter-dependency, any particular capability will play a role that is dependent on the scenario, the context and the presence or absence of other capabilities. This makes it untenable to ascribe an intrinsic value to any capability. Capabilities should instead be assessed in packages. Such packages play key roles in delivering security functions such as detection or response but, ultimately, the value of a capability package should be determined according to the ability of the security layer to which it belongs, to reduce risk. Using the SiD security layer construct makes it possible to gain meaningful assessments of the risk reduction generated by a package of capabilities in a given context (pathway), and thereby a means to assess benefit-cost.

Our third departure was to provide a robust means to identify which of the capabilities or packages should be considered critical to risk reduction efforts on a per-pathway basis, and then how those insights should be aggregated in order to determine strategic priorities for capability enhancement or acquisition. We argue that it is important to generate an appropriate balance across the spectrum of risk pathways representing threats and potential outcomes, because artefacts of an unintended emphasis, for example, on cyber scenarios relative to organised crime, can easily carry through to unbalance assessment of priorities and resource allocations.

We have applied, and subsequently enhanced the approach from our work supporting one of Australia's strategic agencies. Despite its stronger and more defensible methodology, there remain limitations in our approach and significant barriers to its adoption. Not the least of the barriers is the inertia represented in the simplicity and wide adoption of current methods. More importantly, however, the complexity of national security issues dictates that their translation into useful pathways is likely to demand significant time. One advantage of the biannual Dutch process is its evolutionary refinement, based on accumulation of knowledge about the system. Risk pathways provide a similar mechanism for building and representing the knowledge, insights and opinions of agencies and experts. Mining 'data' of this kind and, if appropriate, commissioning new targeted research to understand and refine the pathways should be a requirement of each iteration of national

assessment. In the end, our understanding of the problem is our most important asset for effective risk-informed capability prioritisation.

Rick Nunes-Vaz is Head of the Strategic Security Risk Analysis (SSRA) group in the Joint & Operations Analysis Division of the Defence Science & Technology Organisation, where he leads research to inform strategic decisions in national security, for Defence and non-Defence clients. Rick.Nunes-Vaz@dsto.defence.gov.au

Steven Lord is a Research Scientist in the SSRA Group of DSTO. He uses quantitative robust risk analysis techniques to support operational and strategic decision making. Published security risk research includes analysis of airport front-of-house and the optimisation of controls for security-in-depth. Steven.Lord@dsto.defence.gov.au

Daniel Bilusich is a Research Scientist in the SSRA Group of DSTO. He works on the analysis and implications of strategic risks to Australia's national security from a range of threats, supporting understanding of treatment option priorities. Daniel.Bilusich@dsto.defence.gov.au