RSIS COMMENTARIES (80/2007)

RSIS Commentaries are intended to provide timely and, where appropriate, policy relevant background and analysis of contemporary developments. The views of the authors are their own and do not represent the official position of the S.Rajaratnam School of International Studies, NTU. These commentaries may be reproduced electronically or in print with prior permission from RSIS. Due recognition must be given to the author or authors and the S. Rajaratnam School of International Studies, Nanyang Technological University. For more information on this, please do not hesitate to email: RSISPublication@ntu.edu.sg or call 6790 6982 to speak to the Editor of RSIS Commentaries.

A Risk-based Approach for Homeland Security

Tay Thiam Chye[*]

26 July 2007

THE RECENT foiled plot in the United Kingdom highlighted the reality of homeland security threats. Despite having numerous countermeasures in place and good intelligence, the terrorists still managed to conduct a near successful attack. This incident highlights a fundamental nature of homeland security – states' vulnerabilities are infinite, and the states cannot protect every place, every time. As such, homeland security policymakers need to prioritize their policy goals and allocate the finite resources efficiently. But before this can happen, the critical step of determining the risks arising from threats and vulnerabilities must be taken. The determined risks will then form the basis for subsequent decision-making.

The Twin Homeland Security Challenges

Two inherent homeland security challenges make a risk-based approach to homeland security policy-making necessary. First, the uncertain and complex threat environment arising from highly adaptive adversaries. These adversaries (e.g., terrorists) react to states' anti-terrorism measures by seeking alternative state vulnerabilities. For instance, an anti-terrorism measure that works at the time of introduction may not be effective because of adversary adaptation. Second, the threatened system, i.e., the state, comprises multiple interdependent sub-systems like the economy, social sector and infrastructure. As such, multiple vulnerabilities exist for adversaries to exploit and the consequences of a successful terrorist attack in a sub-system can have cascading effects on the other sub-systems.

Consequently, two key questions for homeland security policy-making arise: Is the government investing enough to generate adequate national security or investing too much at the expense of other public goods that are beneficial for the populace? How cost-effective are the current homeland security policies? Without robust and coherent risk assessment, states may spend too much to protect against high consequence-low probability threats (e.g., September 11), at the expense of protecting against low consequence-high probability threats (e.g., London bombings in July 2005). Consequently, a net security effect for the state may not be created despite huge homeland security investments. This is because a state's increased protection of a particular sector may lead to terrorists targeting other lesser protected sectors.

Risk-based Approach and Risk Assessment

Before such challenges can be addressed, a risk assessment must be carried out to determine the nature and level of risk. This process is embedded in the larger risk-based approach to strategic policy-making. Risk is defined by the *Society for Risk Analysis* as “the potential for realization of unwanted, adverse consequences to human life, health, property, or the environment”.

This commentary focuses on strategic risk assessment whereby risk is assessed systematically across different sectors. Homeland security risk assessment is fundamentally different from traditional risk assessment approaches because the adversary in homeland security is highly adaptive and innovative. While traditional risk assessment processes in industries (e.g., nuclear plants) focuses on “what can go wrong”, homeland security risk assessment focuses on “how can someone make something go wrong”. Thus, instead of focusing only on the possible threats, homeland security risk assessment must also identify plausible threats.

Example: Risk-based Approach for Strategic Early Warning

A risk-based approach can enhance strategic early warning. Risk-based techniques like event trees and fault trees can be used to identify the possible and plausible scenarios based on threats, vulnerabilities, and potential consequences. Subsequently, risks associated with the scenarios are determined. With these as filters, probabilistic models will extract relevant data from large databases. Bayesian network models then postulate the different conditional probabilities of different scenarios while simulation tools analyze “what if” scenarios. These analyses are made more rigorous by qualitative techniques like Red Teaming. Consequently, an effective intelligence cycle is formed because once the possible scenarios are identified, resources can be allocated efficiently and effectively for intelligence collection, analysis, and anticipation. This forms the basis for dynamic and robust strategic early warning.

Implications

Risk has always been part of the policy-making processes in homeland security agencies but it needs to be more institutionalized – the processes must be more explicit, systematic, and integrated. Thus, there are three implications for homeland security policymakers:

- A comprehensive and systematic strategic risk assessment is needed for efficient and effective homeland security policy-making. This process entails prioritization of homeland security policy goals, followed by a detailed risk assessment that assesses the threats, vulnerabilities, and potential consequences. With the risks defined, policy makers have to devise risk management measures to reduce risks. These steps in turn form a basis to compare available risk reduction options by focusing on the trade-offs and their impacts on future options. This risk assessment process must be dynamic and iterative, coupled with a clear understanding of risks for the different stakeholders.

- No single tool can produce a comprehensive risk assessment to cover the whole spectrum of homeland security risks, hence a mixture of qualitative and quantitative methods is needed. Specifically, modelling must be the basis for risk assessment because it provides a structured means to organize and analyze the problem.

- Strategic risk assessment and operational risk assessment must be differentiated. Strategic risk assessment seeks to identify the possible and plausible scenarios for risk monitoring; operational risk assessment seeks to identify the risks associated with specific threats and vulnerabilities. The former provides the greater context for operational risk assessment to assess and act.

In short, while a risk-based approach is not the only way for efficient and effective homeland security policy-making, it is the necessary first step. With the institutionalization of a risk-based approach in the policy-making processes, homeland security agencies will be better prepared to handle new risks and strategic surprises.

[*] *Tay Thiam Chye is an Associate Research Fellow at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University.*