INSTITUTE FOR DEFENSE ANALYSES

A Comparison of Selected Risk Approaches for National Security Decisions

James Thomason
Jim Bexfield
Jason Dechant

June 2019

IDA Document NS D-10726
Log: H 19-000320

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

Distribution authorized to U.S. Government agencies and their contractors; Administrative or Operational Use, June 4, 2019. Other requests for this document shall be referred to OUSD (AT&L)/ARA/EI & OSD Studies.

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication
The work was conducted by the Institute for Defense Analyses (IDA) under CRP C6516.

For More Information:
Mr. Jim N. Bexfield, Project Leader, SFRD
jbexfield@ida.org, 703-258-2778
ADM John C. Harvey, Jr., USN (Ret), Director, SFRD
jharvey@ida.org, 703-575-4530

Distribution authorized to U.S. Government agencies and their contractors; Administrative or Operational Use, June 4, 2019. Other requests for this document shall be referred to OUSD (AT&L)/ARA/EI & OSD Studies.

INSTITUTE FOR DEFENSE ANALYSES

IDA Document NS D-10726

A Comparison of Selected Risk Approaches for National Security Decisions

James Thomason
Jim Bexfield
Jason Dechant

Distribution authorized to U.S. Government agencies and their contractors; Administrative or Operational Use, June 4, 2019. Other requests for this document shall be referred to OUSD (AT&L)/ARA/EI & OSD Studies.

This page is intentionally blank.

Distribution authorized to U.S. Government agencies and their contractors; Administrative or Operational Use, June 4, 2019. Other requests for this document shall be referred to OUSD (AT&L)/ARA/EI & OSD Studies.

Executive Summary

MORS Presentation: **A comparison of selected risk approaches for national security decisions**

Authors: Dr. James Thomason (IDA), Mr. Jim Bexfield (IDA), FS, Dr. Jason Dechant (IDA)

The use of risk analysis to support major decisions has increased over the years in the national security community. Examples include the development of a Mission Risk Register in the Department of Homeland Security (DHS), an optimization model supporting the defense industrial base in the Office of the Secretary of Defense (OSD), the use of the Integrated Risk Assessment and Management Model (IRAMM) to support the Commission on the Future of the Army, and the annual risk assessment prepared by the Chairman of the Joint Chiefs of Staff. This presentation briefly describes four risk-analytic applications that were presented in an IDA-hosted event titled "Senior-Level Forum on the Use of Risk to Improve National Security Decisions." The forum was held on December 14, 2018, and was attended by members of the Joint Staff and Department of Homeland Security. The description of the four methods is followed by a comparison using several attributes. The IDA presentations are:

- Developing a Department of Homeland Security Mission Risk Register (Dr. Jason Dechant)
- Managing Force Structure Under Uncertainty: The Stochastic Active and Reserve Affairs (SARA) Model (Dr. Nancy Huff)
- Munitions Optimization (MunOpt) Model to Support OSD (Dr. Dan Lago and Ms. Julie Kelly)
- Potential Applications of the Integrated Risk Assessment and Management Model (IRAMM) (Mr. James Bexfield and Dr. James Thomason)

Below is a comparison of the four approaches.

Distribution authorized to U.S. Government agencies and their contractors; Administrative or Operational Use, June 4, 2019. Other requests for this document shall be referred to OUSD (AT&L)/ARA/EI & OSD Studies.

IDA | Comparison of Approaches

	Alternative Methods			
Area	Mission Risk Register	SARA	MunOpt	IRAMM
Uses a consequence scale	yes	no	no	yes
Uses a complex model	no	yes – accounting model	yes - optimizer	no
Extent of decision maker involvement	extensive	some	some	extensive
Explicitly includes cost	no	yes	yes	no
Risk measurement	score that ranges from 1-5	shortfall in meeting deployment needs	unmet demand & readiness gaps	sum of consequence score times probability
Generate options for mitigating risk	some	some	some	major focus

27

The presentation concludes with some recommendations on ways to improve the use of risk concepts in the national security arena. The recommendations include:

- Build an understanding of alternative approaches to risk
- Gain acceptance of a risk lexicon (and perhaps taxonomy)
- Foster better collaboration across communities (DOD and DHS, academia and practitioners, etc.)
- Educate decision makers in the best ways to use risk
- Develop metrics on the extent to which risk is considered in national security decisions (and identify approaches that have been used often)
- Develop a guide for best practices across the risk analytic community that differentiates according to application

IDA

A Comparison of Selected Risk Approaches for National Security Decisions

June 2019

Dr. James Thomason, Mr. Jim Bexfield, FS, Dr. Jason Dechant

Institute for Defense Analyses

IDA

What is Risk?

1] "The possibility of loss or injury" -- Merriam Webster Dictionary

2] "(Exposure to) the possibility of loss, injury, or other adverse or unwelcome circumstance; a chance or situation involving such a possibility" -- Oxford English Dictionary

Common Aspects of Risk Definitions
- Possibility of occurrence
- Adverse effects/consequences

Some implications…..

The greater the possibility (chance) of a loss, the greater the risk	The greater the possible loss or injury (adverse consequences, costs) the greater the risk

2

IDA

Selected Major Applications:
Risk Supporting National Security Decisions

- Department of Defense (DOD): The Department routinely engages in various risk assessments. A leading example: The Chairman's Risk Assessment (CRA)
  - Required by Congress, including the submission of mitigation plans for all significant risks
  - Joint Risk Assessment methodology (see Chairman of the Joint Chiefs of Staff Memorandum (CJCSM) 3105.01, 14 Oct 2016)
- Department of Homeland Security (DHS): Cybersecurity and Infrastructure Security Agency (CISA) identifies, analyzes, prioritizes, and manages high-consequence threats to critical infrastructure through a crosscutting risk-management paradigm
  - National Risk Management Center measures risk

3

IDA

Some Major Initiatives to Improve the Use of Risk

- Society activities
  - MORS
    - Risk Analysis Community of Practice (CoP) led by Dr. Arch Turner
    - Risk Analysis in National Security continuing education course (5 days)
  - Security Analysis and Risk Management Association (SARMA)
- Academia
  - George Mason University: Decision and Risk Analysis
  - Old Dominion University: Computational Risk Modeling & Decision Analytics research area
- Others…

4

IDA

Brief Descriptions of Four Risk Methods

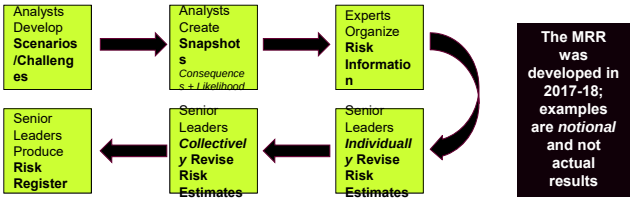
- Methods
  - Department of Homeland Security Mission Risk Register (Dr. Jason Dechant)
  - The Stochastic Active and Reserve Affairs (SARA) Model (Dr. Nancy Huff)
  - Munitions Optimization (MunOpt) Model (Dr. Dan Lago and Ms. Julie Kelly)
  - Integrated Risk Assessment and Management Model (IRAMM) (Mr. James Bexfield and Dr. James Thomason)

5

IDA

Homeland Security Mission Risk Register

- **Approach**
  - **Quantitatively** estimate strategic risks for designated high-priority Challenge Areas (expressed as scenarios) in the context of a specific U.S. force structure
  - Capture **qualitative** comments that provide respondents' justification and rationales for their quantitative risk scores
  - Combining the results of **both** to stimulate group discussions used to finalize risk register
- **Results used** to inform resourcing decisions and strategic planning



IDA

Challenge Areas:
MRR Scenario Space

33 scenarios, provided by DHS, derived from Homeland Security National Risk Characterization

Chemical / Biological – 6 scenarios
- Agricultural Plant Disease
- Biological Attack in a Crowded Infrastructure Environment
- Chemical Attack Leveraging VBIED to release Chemicals in Situ
- Chemical Attack Using Stolen Chemicals
- Foreign Animal Disease
- Transnational Communicable Human Disease

Technological Attacks – 11 scenarios
- Covert Manipulation of Government Data
- Cyber Attack Disrupting an Internet Backbone
- Cyber Attack on Election Systems
- Cyber Attack on Infrastructure Asset Operations
- Cyber Attack on Infrastructure System Operations
- Cyber Attacks on Shared Infrastructure
- Cyber Theft of Sensitive Information
- Denial of Emergency Communications
- Information Warfare against the United States
- Insider Theft of Extremely Sensitive Information
- Sabotage of Key Communications Infrastructure

Easily Obtained Arms – 2 scenarios
- Unsophisticated Attacks at Open/Low Security Venues
- Unsophisticated Attacks at Venues with Perimeter Security

Manned and Unmanned Aircraft Vehicles - 2 scenarios
- Aircraft Used as Weapons
- UAS Attacks

Natural Hazards - 7 scenarios
- Droughts
- Earthquakes
- Flooding
- Hurricanes
- Tsunamis
- Volcanoes
- Wildfires

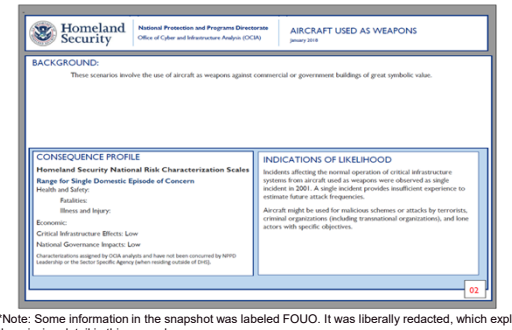
Nuclear, Radiological Attacks, and EMP – 3 scenarios
- Electromagnetic Pulse / Geomagnetic Disturbances
- Nuclear Attacks
- Radiological Attacks

Vehicle-Borne Improvised Explosive Device – 2 scenarios
- VBIED Attack at a Secured Facility
- VBIED Attack at an Open, Unsecured Venue

7

IDA

Risk Snapshots:
Consequences and Likelihood Added to Scenarios to Create Snapshots*



Homeland Security | National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis (OCIA) | AIRCRAFT USED AS WEAPONS | January 2018

BACKGROUND:

These scenarios involve the use of aircraft as weapons against commercial or government buildings of great symbolic value.

CONSEQUENCE PROFILE

Homeland Security National Risk Characterization Scales
Range for Single Domestic Episode of Concern
Health and Safety:
Fatalities:
Illness and Injury:
Economic:
Critical Infrastructure Effects: Low
National Governance Impacts: Low

Characterizations assigned by OCIA analysts and have not been concurred by NPPD Leadership or the Sector Specific Agency (when residing outside of DHS).

INDICATIONS OF LIKELIHOOD

Incidents affecting the normal operation of critical infrastructure systems from aircraft used as weapons were observed as single incident in 2001. A single incident provides insufficient experience to estimate future attack frequencies.

Aircraft might be used for malicious schemes or attacks by terrorists, criminal organizations (including transnational organizations), and lone actors with specific objectives.

02

*Note: Some information in the snapshot was labeled FOUO. It was liberally redacted, which explains the missing detail in this example.

8

IDA

Risk Snapshots:

Consequence Scales Used to Convey Data

Common consequence scales used to convert snapshot data into ordinal scales

	Economic	Essential Infrastructure Effects	National Governance Impacts	Health & Safety
Very High	National economic impacts, causing business disruption, cleanup, and restoration costs. Over $100B	Broad-reaching outages of lifeline infrastructure that leave major productive areas offline for over a month	Multiple complex failures lead to a crisis of confidence in Government and societal institutions.	Event causes directly attributable deaths, with illness injuries in the millions Over 100,000 deaths
High	Very disruptive and destructive within multiple cities or a large region, causing business disruption, cleanup, and restoration costs $10B - $99B	Significant outages of lifeline infrastructures across multiple cities or a large region that last for up to a month.	Many Agencies are affected by the event in such a way as to be unable to fulfill mission essential functions	Greater than Nationally critical losses 10,000 to 99,999 deaths
Moderate	Very disruptive and destructive within multiple cities or a large region, causing business disruption, cleanup, and restoration costs $1B - $9.9B	Outages of lifeline infrastructures across multiple cities or a large region, up to a week	Agencies are affected by the event in such a way as to be unable to fulfill mission essential functions	Regionally to nationally critical losses 1,000 to 9,999 deaths
Low	Disruptive and destructive within a city, causing business disruption, clean up and restoration costs $100 M to $999M	Significant local outages of lifeline infrastructures, up to 2 days	Many individuals who are in positions of public trust are unable to do their duty	Very Significant casualties, beyond what can be managed with planned resources 100 to 999 deaths
Very Low	Disruptive and destructive for a major company, or a portion of an city or economically important area. Less than $100M	Localized outages of lifeline infrastructures lasting less than a day	Limited impact on governance and public confidence	Significant but manageable casualties Fewer than 100 deaths

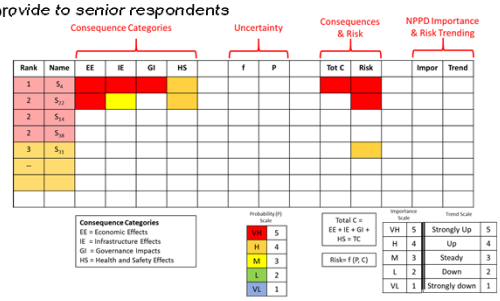
9

IDA

Organize Risk Information:

Analysts Organize Information to Present to Senior Respondents

Experts assign risk scores to all categories except Importance and Trends and *provide to senior respondents*



10

IDA

Respondent Individual Assessment:

Senior Leaders Adjust/Defend Risk Estimates to Create Risk Profile

- Senior leaders interviewed individually to provide risk estimates
- In advance of interviews, respondents provided:
  - Scenario descriptions
  - Exercise description
- During interview, respondents provided snapshots and pre-binned list of scenarios
- Respondents asked to:
  - Adjust risk rankings
  - Provide rationale (including probability and consequences)
  - Indicate Importance and Trend

Notional Example of Pre-Binned Risk Information

A-1			Senior Leader MRR - IDA Compilation
Q #	Rank	Scenario Class	Scenario
22	1	Nuk/Rad/EMP	Nuclear Attacks
25	4	Chem/Bio	Transnational Communicable Human Disease
20	10	Tech	Information Warfare against the United States
10	1	Tech	Cyber Attack on Infrastructure System Operations
11	1	Tech	Cyber Attacks on Shared Infrastructure
19	4	NatHaz	Hurricanes
3	6	Chem/Bio	Biological attack in a crowded infrastructure environment
12	7	Tech	Cyber Theft of Sensitive Information
15	7	NatHaz	Earthquakes
17	7	NatHaz	Flooding
28	10	Easily/IA-Are	Unsophisticated Attacks at Open/Low-Security Venues
24	10	VBIED	VBIED Attack at an Open, Unsecured Venue
9	11	Tech	Cyber Attack on Election Systems
21	14	Tech	Insider Theft of Extremely Sensitive Information
24	13	Tech	Sabotage of Key Communications Infrastructure
14	12	Nuk/Rad/EMP	Electromagnetic Pulse / Geomagnetic Disturbances
5	13	Chem/Bio	Chemical attack using stolen chemicals
7	14	Tech	Cyber Attack disrupting an Internet Backbone
14	12	NatHaz	Droughts
26	16	NatHaz	Tsunamis
8	13	Tech	Cyber Attack on Infrastructure Asset Operations
30	13	NatHaz	Wildfires
2	11	Mnv/Un A1	Aircraft Used as Weapons
23	11	Nuk/Rad/EMP	Radiological Attacks
29	11	Easily/IA-Are	Unsophisticated Attacks at Venues with Perimeter Security
4	16	Chem/Bio	Chemical attack leveraging VBIED to release chemicals in situ
27	16	Mnv/Un A1	VAB Attacks
32	16	NatHaz	Volcanoes
30	30	VBIED	VBIED Attack at a Secured Facility
6	31	Tech	Covert Manipulation of Government Data
18	16	Chem/Bio	Foreign Animal Disease
13	32	Tech	Denial of Emergency Communications
1	33	Chem/Bio	Agricultural Plant Disease
34	34	Nuk/Rad/EMP	GeoMagnetic Disturbances - 2

11

IDA

Senior Leader Forum:

Senior Leaders Collectively Revise Risk Estimates

- All senior respondents convened to develop final risk register
- Provided with:
  - Individual assessments for reference
  - Aggregated assessment (based upon highest rating for each scenario)
- Results presented to the group; chair-led discussion (final authority)
  - Areas of closest agreement and greatest divergence presented
- The group collectively agreed to risk in each scenario resulting in a final ranking—the Mission Risk Register

A-2			Senior Leader MRR - IDA Compilation	Risk By Respondent									Total Risk					
Q #	Rank	Scenario Class	Scenario	R1	R2	R3	R4	R5	R6	R7	MAX	SUM	VH	H	M	L	VL	R
22	1	Nuk/Rad/EMP	Nuclear Attacks									26	2	2	2	1		
25	4	Chem/Bio	Transnational Communicable Human Disease									24	1	2	3	1		
20	10	Tech	Information Warfare against the United States									28	1	1	2	2	1	
10	1	Tech	Cyber Attack on Infrastructure System Operations									26		5	2			
11	1	Tech	Cyber Attacks on Shared Infrastructure									26		5	2			
19	4	NatHaz	Hurricanes									24		3	4			
3	6	Chem/Bio	Biological attack in a crowded infrastructure environment									22		1	6			
12	7	Tech	Cyber Theft of Sensitive Information									23		2	3	2		
15	7	NatHaz	Earthquakes									23		1	5	1		

Notional Example

12

IDA

Mission Risk Register:

Forum Produces Risk Register

The senior leader forum produced the 2017/2018 DHS Mission Risk Register

2018 Scenario Type	Risk Score
Scenario xx	5
	4
	4
	4
	4
	4
	4
	4
	4
	4
Scenario yy	4

2018 Scenario Type	Risk Score
Scenario zz	3
	3
	3
	3
	3
	3
	3
	3
	3
	3
	3
Scenario tt	3

2018 Scenario Type	Risk Score
	2
	2
	2
	2
	2
	2
	2
	2
	2
	2
	2

13

IDA

The SARA Model

Structure and Readiness Assessment

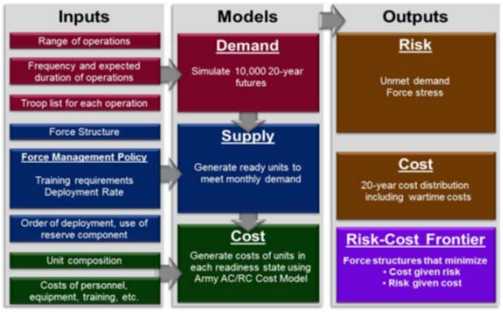
(SARA assesses cost and risk tradeoffs at the unit level)

- Generates **readiness** at the **unit level**
- Calculates **costs** based on **resourcing and use**
- Calculates **force sufficiency** under a wide range of **specified or uncertain** operational requirements

14

IDA

SARA Model Overview

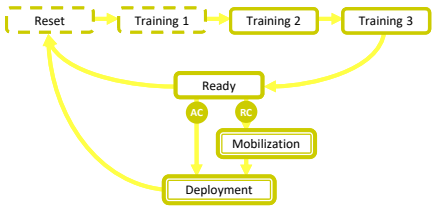


15

IDA

Specify the Planned Rotation Rate by Unit and Component

Total time in reset and training defines the **dwell period**



16

IDA

The Demand Generator Simulates 10,000 Futures

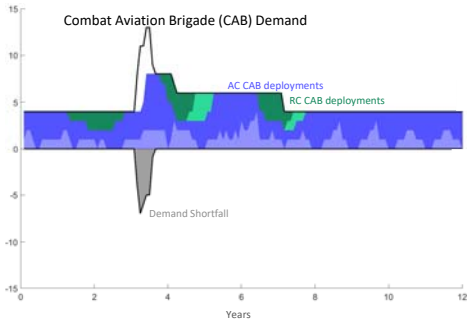
- **Operation Inputs**
- Frequency
- Stages
  - Duration (fixed or uncertain)
  - Troop list

- **Demand Generator**
- Simulate 10,000 20-year futures

17

IDA

The Supply Model Tracks Deployments and Shortfalls



18

IDA

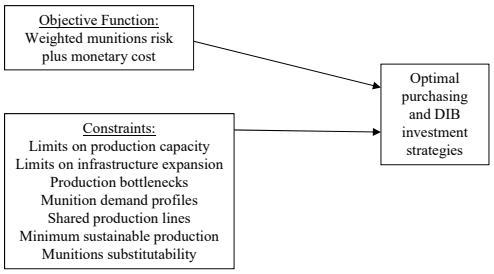
Munitions Optimization (MunOpt) Model

- Problem: Determine best munition investment plan
  - Purchases to replenish munitions used in the steady state (counter-terrorism activities, test and training)
  - Optimal production schedule that considers production lead times and munitions that share production lines
  - Infrastructure investments needed to either enhance existing facilities or build new plants to increase capacity
    - Both prime and sub-tier supply capabilities are considered
  - Purchases that prepare for munition surges resulting from unexpected major conflicts
- Risk concept: negative outcomes associated with insufficient munition stockpiles

19

IDA

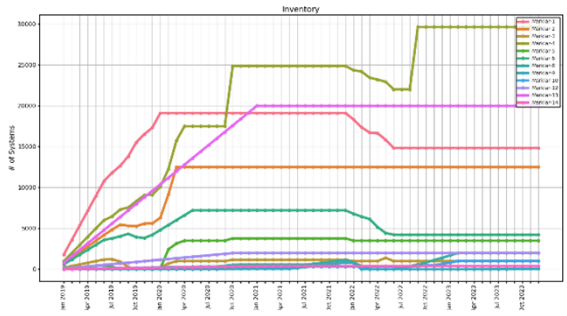
MunOpt Linear program



20

IDA

Notional MunOpt Output: Inventory Over Time



21

IDA

Integrated Risk Assessment and Management Model (IRAMM)

- Calculates risk based on
  - Probability of adverse event(s) occurring
  - Consequences if the event(s) occurs
- Uses strong (ratio-level) consequence scales to promote consistency and enable comparisons
- Interviews with decision makers elicit quantitative assessments and supporting rationales
- Candid group discussions foster understanding, convergence, identification of mitigating alternatives, and stronger teamwork

22

IDA

The IRAMM Interview (1.5–2 hours)

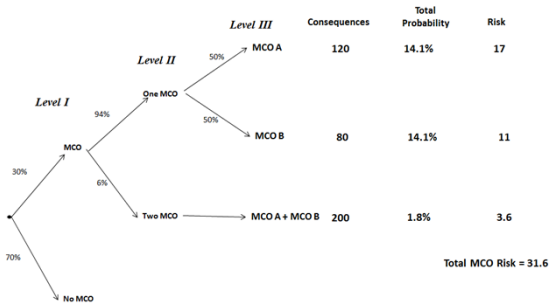
- Introduction by interviewer
  - Definitions of the challenge areas (MCOs, HLD, Irregular warfare)
  - Summary of the U.S. and allied forces that may be available to respond to an adversary
  - Introduction to the consequence tools
- Respondent specifies scenarios for first challenge area and for each scenario identifies the following:
  - Who the players are (countries, organizations, and so forth)
  - How it starts
  - Possible key events (including results of conflicts),
  - How it may end, and so forth
- Respondent estimates the probabilities and begins building an event tree

Consequence Scale

23

IDA

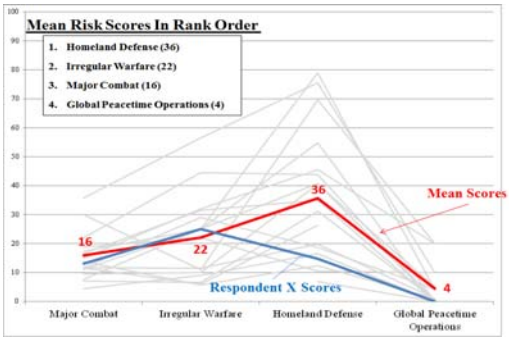
Event Tree with Risk for MCO Challenge Area



24

IDA

Respondent Score Compared to Mean and Scores of Others



25

IDA

Alternative Viewpoints: Homeland WMD Attack

	Greater Risk Viewpoint	Lesser Risk Viewpoint
1	An individual or organization with intent to attack the U.S. with a nuclear, biological, or radiological weapon could succeed, and there could be significant psychological effects. The resultant domestic *political consequences* could threaten the federal structure of our government	There is a "negligible chance" that a radiological or chemical attack would occur, and, in the event one did, the consequences would be "negligible"
2	The consequences of a significant terrorist-initiated biological event had the potential to be "surprisingly" close to those of a nuclear detonation as the result of the disruption of our way of life and the suppression of the *economy* following the breakout of a vector-borne illness. The probability of a radiological attack is much higher than that of a nuclear attack, but the consequences would be almost as severe	A biological attack would most likely be conducted by a disgruntled domestic who is not particularly sophisticated. The consequences would be small and contained, consisting of possibly "giving up some liberties"
3	There is an 80% chance that a nuclear weapon is detonated in the United States in the coming decade. With regard to a nuclear attack, there is a serious threat (e.g., emanating from Pakistan, of proliferation to small groups, and insufficient capacity to detect devices coming into the United States)	Nuclear attack would require a lot of things to have to come together. It is too difficult for someone to detonate a nuclear device on the homeland. Our enemies are not sophisticated enough to obtain, create, or deliver such weapons

26

IDA

Comparison of Approaches

	Alternative Methods			
Area	Mission Risk Register	SARA	MunOpt	IRAMM
Uses a consequence scale	yes	no	no	yes
Uses a complex model	no	yes – accounting model	yes - optimizer	no
Extent of decision maker involvement	extensive	some	some	extensive
Explicitly includes cost	no	yes	yes	no
Risk measurement	score that ranges from 1-5	shortfall in meeting deployment needs	unmet demand & readiness gaps	sum of consequence score times probability
Generate options for mitigating risk	some	some	some	major focus

27

IDA

Challenges

- What is the best way of improving the use of risk concepts in the national security arena?
  - Build an understanding of alternative approaches to risk
  - Gain acceptance of a risk lexicon (and perhaps taxonomy)
  - Foster better collaboration across communities (DOD and DHS, academia and practitioners, etc.)
  - Educate decision makers in the best ways to use risk
  - Develop metrics on the extent to which risk is considered in national security decisions (and identify approaches that have been used often)
  - Develop a guide for best practices across the risk analytic community that differentiates according to application
- Should MORS stand up a working group focused on the measurement and use of risk in decision making?

28

IDA | Questions and contact information

- Dr. James Thomason (jthomaso@ida.org)
- Mr. Jim Bexfield (jbexfield@ida.org)
- Dr. Jason Dechant (jdechant@ida.org)

29

This page is intentionally blank.

Distribution authorized to U.S. Government agencies and their contractors; Administrative or Operational Use, June 4, 2019. Other requests for this document shall be referred to OUSD (AT&L)/ARA/EI & OSD Studies.