

ASSESSING TERRORIST CYBER THREATS:
ENGINEERING A FUNCTIONAL CONSTRUCT

Deanne Morgan, BSc, BS, MS

Dissertation Prepared for the Degree of
DOCTOR OF PHILOSOPHY

UNIVERSITY OF NORTH TEXAS

December 2014

APPROVED:

Brian C. O'Connor, Major Professor
Bradley S. Chilton, Committee Member
Ahmet S. Yayla, Committee Member
Suliman Hawamdeh, Chair of the Department of Library and Information Sciences
Mark Wardell, Dean of the Graduate School

Morgan, Deanne. *Assessing terrorist cyber threats: Engineering a functional construct*. Doctor of Philosophy (Information Science), December 2014, pp. 133 pp., 10 tables, references, 40 titles.

Terrorist organizations and individuals make use of the Internet for supportive activities such as communication, recruiting, financing, training, and planning operations. However, little is known about the level of computer-based (“cyber”) threat such terrorist organizations and individuals pose.

One step in facilitating the examination and assessment of the level of cyber threat posed by terrorist organizations and individuals is development of an assessment tool or methodology. This tool would guide intelligence collection efforts and would support and facilitate comparative assessment of the cyber threat posed by terrorist organizations and individuals through the provision of a consistent method of assessment across time, amongst organizations and individuals, and between analysts.

This study leveraged the professional experience of experts to engineer a new functional construct – a structured analytical technique designed to assess the cyber threat posed by terrorist entities and individuals. The resultant instrument was a novel structured analytical construct that uses defined indicators of a terrorist organization/individual’s intent to carry out cyber attacks, and their capability to actually do so as measures of an organization/individual’s overall level of cyber threat.

Copyright 2014

By

Deanne Morgan

ACKNOWLEDGEMENTS

Thank you to my committee members for your patience and support. Your insights and encouragement have been invaluable.

I am grateful for the patience, encouragement, support, advice, and consultation provided by my manager and colleagues, as well as others who have touched my path as I navigated this journey. The study's participants encouraged and inspired me in innumerable ways. My editor/proofreader stood by me and offered helpful suggestions. Although you cannot be named individually, know that your assistance has been invaluable. Thank you.

Finally, thank you to my employer for being supportive of me conducting this study, and to the employers and managers of my participants, who gave permission for their employees to participate.

TABLE OF CONTENTS

| | Page |
|--|------|
| ACKNOWLEDGEMENTS..... | iii |
| LIST OF TABLES..... | viii |
| Chapters | |
| 1. INTRODUCTION..... | 1 |
| Justification..... | 1 |
| Significance..... | 2 |
| Theoretical Background..... | 3 |
| Terrorist Individuals and Organizations: A Complex Threat..... | 3 |
| Mixed-Methods Approach..... | 5 |
| Intelligence-led Policing..... | 6 |
| Interdepartmental Expert Groups..... | 7 |
| Intelligence Analytical Methods..... | 8 |
| Project Sleipnir: Background..... | 9 |
| Project Sleipnir: Concepts..... | 10 |
| Project Sleipnir: Attributes..... | 10 |
| Assumptions..... | 12 |
| 2. RELATED LITERATURE..... | 13 |
| Terrorist Use of Information Technology..... | 15 |
| Adoption of Information Technology..... | 18 |
| Threat Posed by Terrorists and Terrorist Organizations..... | 21 |

| | |
|---|----|
| Threat Assessments..... | 23 |
| Indicators of Terrorist Behavior..... | 27 |
| 3. METHODS..... | 30 |
| Introduction..... | 30 |
| Research Participants..... | 31 |
| Participant Demographics..... | 32 |
| Information Needed to Conduct the Study..... | 35 |
| Overview of Research Design..... | 36 |
| Prototype Analytical Tool Instrument Creation..... | 38 |
| IRB Approval..... | 39 |
| Data Collection Methods..... | 39 |
| Phase One: Revision of the Prototype Analytical Tool Instrument..... | 39 |
| Phase Two: Reworking of the Revised Analytical Tool Instrument..... | 40 |
| Phase Three: Focus Group..... | 41 |
| Data Analysis Methods..... | 43 |
| Ethical Considerations..... | 43 |
| Issues of Trustworthiness..... | 45 |
| Limitations of the Study..... | 45 |
| Summary..... | 47 |
| 4. RESULTS..... | 48 |
| Revision of the Prototype Analytical Tool..... | 48 |

| | |
|---|----|
| Reworking of the Revised Analytical Tool..... | 48 |
| General Discussion About the Tool..... | 48 |
| Introduction and Instructions on How to Use the Tool..... | 49 |
| Indicators..... | 50 |
| Unknowns..... | 53 |
| Focus Group..... | 54 |
| General Discussion..... | 54 |
| An Expert-Based Scientific Structured Analytical Technique..... | 55 |
| The Narrative..... | 56 |
| The Instrument..... | 57 |
| The Indicators..... | 59 |
| Threat Table..... | 60 |
| Validation of the Instrument: Vignette Assessments..... | 61 |
| Final Questionnaire..... | 63 |
| 5. CONCLUSION..... | 67 |
| Structure..... | 67 |
| Indicators..... | 68 |
| Additional Material..... | 69 |
| Validation..... | 69 |
| The Future..... | 70 |
| APPENDIX A: PROTOTYPE ANALYTICAL TOOL INSTRUMENT..... | 72 |
| APPENDIX B: REVISED ANALYTICAL TOOL INSTRUMENT..... | 84 |
| APPENDIX C: FICTIONAL VIGNETTES..... | 96 |

| | |
|---|-----|
| APPENDIX D: FINAL ANALYTICAL TOOL INSTRUMENT..... | 101 |
| REFERENCES..... | 130 |

LIST OF TABLES

| | Page |
|--|------|
| 2.1 Modes of Information Technology Use by Terrorists..... | 16 |
| 2.2 Physical Threat Analysis Methodology..... | 24 |
| 2.3 CRTI's CRA Risk Matrix Table..... | 26 |
| 2.4 CRTI's CRA Preparedness Prioritization Matrix | 26 |
| 3.5 Combined Total Years of Experience in Specified Areas of Work..... | 35 |
| 3.6 Total Years of Experience per Specific Relevant Areas of Work..... | 35 |
| 4.7 Indicators: Changes and Comments..... | 60 |
| 4.8 Threat Table Colors..... | 61 |
| 4.9 Individual Vignette Assessment Results..... | 62 |
| 4.10 Results of Group Assessment of Vignettes..... | 64 |

CHAPTER ONE

INTRODUCTION

This study developed a new functional construct: a qualitative analytical technique designed to assess the cyber threat posed by terrorist organizations and individuals. The final instrument is a novel structured analytical construct that uses defined indicators of a terrorist organization/individual's intent to carry out cyber attacks, and their capability to actually do so as measures of an organization/individual's overall level of cyber threat.

Justification

Terrorist organizations and individuals make use of the Internet for supportive activities such as communication, recruiting, financing, training, and operational planning. However, little is known about the level of computer-based ("cyber") threat terrorist organizations and individuals pose.

My Master of Science thesis, *Challenges encountered during law enforcement investigations of terrorist use of information technology* (Morgan, 2005), provided a number of recommendations for further research. The second recommendation within the research and development domain was: "(D)evelop tool(s) for assessing the cyber threat posed by terrorists and/or terrorist organizations."

Based on a review of the available literature, it is my belief that no such tool currently exists. This belief was confirmed in 2005, then again in 2014, through private conversations with a number of professional intelligence analysts, and further confirmed through discussions with this study's participants. Existing tools, such as the Cyber

Threat Metrics by Mateski et al. (2012), either focus on post-incident analysis with a strong or exclusive technical component, and/or do not assess the cyber threat posed by terrorist individuals or organizations. It is expected that the lack of such a methodology limits the robustness, reliability, and consistency with which terrorist cyber threats are assessed. The divergent functional world that exists between the theoretical/academic and practitioner analyst creates a gap where there is insufficient overlap. It is this gap which this study aims to address by engineering a validated functional construct to support analysis.

Significance

This tool will benefit the security and intelligence community by:

- a) Providing a means to consistently assess the relative cyber threat posed by a single terrorist organization or individual.
- b) Providing a means to compare terrorist individuals and organizations against other terrorist individuals and organizations through the use of a standardized method of assessment.
- c) Increasing the validity of inter-assessment comparisons over time.
- d) Increasing the reliability of assessment comparisons between different analysts.

As a result, security intelligence and law enforcement agencies will be able to more reliably assess the threats and potential threats, identify intelligence gaps, support decision-making, and appropriately allocate scarce or limited resources to address the terrorist cyber threat.

Theoretical Background

Terrorist Individuals and Organizations: A Complex Threat

The threat from terrorist individuals and organizations is complex (Bjelopera, 2013), as terrorists are diverse with varying intents and capabilities, and supporting resources and structures (O'Brien, 2011). Vos Fellman and Wright (2004) refer to terrorist networks as “autonomous non-state actors” and “complex, self-organizing systems” which require new models (p. 1). They go on to describe terrorist behavior in the formal properties of a system, arguing that it “falls somewhere between the purely chaotic and the fully deterministic realms, which we represent as a non-linear dynamical system, characterized by a low-order chaotic attractor” (p. 2). Vos Fellman and Wright note the utility of complex system tools in assessing terrorist networks, but caution that some models may be limited as a result of the dynamic nature of terrorist cells.

Krebs' (2002) examination of mapping terrorist networks identified a number of useful issues. One is the contrast in difficulty mapping covert networks before and after an event: “Analyzing networks after an event is fairly easy for prosecution purposes. Mapping covert networks to prevent criminal activity is much more difficult” (p. 43). In the context of applying social network theory, Sparrow's (as cited in Krebs, 2002) “overview of the application of social network analysis to criminal activity” (p. 44), was described, with Krebs noting he also found the same issues, notably:

1. Incompleteness – the inevitability of missing nodes and links that the investigators will not uncover.
2. Fuzzy boundaries – the difficulty in deciding who to include and who not to include.

3. Dynamic – these networks are not static, they are always changing. Instead of looking at the presence or absence of a tie between two individuals, Sparrow suggests looking at the waxing and waning strength of a tie depending upon the time and the task at hand. (p. 44)

These issues are also at play with the development of the functional construct in the current study: when applying the instrument in practice, not all data will be available to analysts (therefore there will be intelligence gaps, incompleteness), there will be difficulties deciding what to include when constructing the instrument, and also what information to include when using it (fuzzy boundaries), and, finally, terrorist individuals and organizations change over time (dynamic), meaning that an assessment performed at a singular point in time may no longer be reflective of the threat posed.

Vos Fellman and Wright (2004) describe Krebs' work as combining "social network analysis and organizational behavior with chaos theory and complex adaptive systems" to examine "knowledge networks within and across the boundaries of an organization in order to uncover the dynamics of learning and adaptation" with identified "communities of practice" (p. 7). Unfortunately, while social network analysis allows insight into how a terrorist network functions, it does not support direct assessment of the level of threat a group poses, the problem at hand for this study. The quantitative nature of social networking analysis does not readily translate into the qualitative nature *in situ*. Further, social network analysis examines only some aspects of capability and intent that contribute to the cyber threat picture.

Mixed-Methods Approach

Developing a functional construct for assessing the cyber threat posed by terrorist individuals and organizations is fundamentally a practitioner problem. No single theoretical model is applicable, as each has boundaries that are artificial in the practitioner's realm. For example, a working practice of analysts is to conduct what is essentially a content analysis of information in order to identify trends, patterns, and key information. The coding used in the analysis is developed by the analysts themselves, typically on an *ad hoc* basis as determined by the specific needs of the particular analysis being conducted. In private conversation with various analysts, I have discovered that most are unaware that the process they are employing would be considered a content analysis within the theoretical environment; within the practitioner's world it is simply one approach among many without a formal name.

Another example is the development of indicators. Although formalized warning analysis techniques using indicator lists exist and are used extensively in domains such as the defense community (Grabo, 2002), analysts without training in warning analysis will also create their own indicators. For example, if an analyst wants to know if a criminal organization is engaging in activity A, they may identify other activities that group would have to be performing in order to be engaged in activity A. These other activities are indicators of activity A. The analyst would then look through the criminal intelligence available to them for these other indicators as part of their assessment of the group's engagement in activity A.

A different type of example of this is the identification of indicators demonstrating pre-incident planning by terrorists. Some of the activities terrorists may undertake

during the planning stages of an attack, such as buying explosives (or the components to make explosives), conducting surveillance of a target, making a dry run, and others, may be observable by others. If observed, reported to authorities and recognized as pre-incident planning steps, it may be possible to intervene and prevent the planned attack. The United States' Nationwide SAR Initiative is premised on this basis (Institute for Intergovernmental Research, 2014).

Development of a viable construct therefore requires a mixed-methods approach that draws on strengths and results from multiple areas to engineer a construct that is functional and can be validated in practice.

For example, the construct draws on lessons learned from the application of social network theory about how terrorist networks are interlinked and the dynamics within their hierarchies. It uses the concepts of defined indicators from the Royal Canadian Mounted Police's (RCMP) Sleipnir model (Strang S. J., 2005) and warning analysis techniques as a cornerstone for its structure. Additionally, it makes use of the general theory approach of starting back at first principles and letting the data lead, in this case from a review of literature, to identify the indicators themselves.

Intelligence-led Policing

Many law enforcement agencies have adopted the principles of intelligence-led policing. Among its many aspects, intelligence-led policing fosters a structured approach to operational decision making. Tactical, operational, and strategic intelligence all play important roles in an intelligence-led police agency (Bureau of Justice Assistance, 2005). For example, the RCMP uses strategic intelligence “to

recommend criminal intelligence and enforcement priorities to the RCMP's senior operational officers" (Strang S. , 2005, p. 1). Cope noted that "the emphasis on knowing and controlling risk in modern societies has influenced techniques of crime control" and "the process of intelligence-led policing exemplifies concerns with identifying, prioritizing and intervening to minimize risk" (2004, p. 190).

Intelligence can be described as processed information used to inform police action. The intelligence process consists of tasking, collection, evaluation, collation, analysis, inference development, dissemination, and re-evaluate, continuing the cycle. (United Nations Office on Drugs and Crime (UNODC), 2011). It takes raw data, turns it into information, and then ultimately transforms it into actionable intelligence by providing value and ascribing relevance.

Analytical tools, techniques, and methods assist these agencies in determining priorities for combating organized crime and terrorism, typically by identifying "the specific criminal organizations posing the greatest threat to ... society, and the key individuals engaged in criminal activity whose investigation, arrest and prosecution would cause the greatest disruption to those groups." (Strang S. , 2005, p. 1). Management is then able to "approve investigative projects and allocate resources to them in order to act on the priorities" (p. 1).

Interdepartmental Expert Groups

The Canadian Intelligence Community uses a venue called Interdepartmental Experts Groups (IEG) as one means of accomplishing a whole-of-government

assessment about issues of concern. While there are few public references to IEGs, Spencer (1996) described IEGs as the following:

“departmental experts on issues of interest to the CIC are brought together in...Interdepartmental Expert Groups (IEG's), which have the principal responsibility for producing finished intelligence. The IEG's can be either ad hoc to meet special requirements, or of a standing character to deal with continuing areas of intelligence concern. A real attempt at consensus is made within IEG's” (p.8).

Strang's development of the Sleipnir technique for the RCMP also made use of expert judgment; within the tool, “the definitions and weights for each attribute set reflect consensus of opinions of individuals from the RCMP and other agencies with expertise in the topic areas. Consensus was achieved by using the Delphi Method” (Strang S. , 2005, p. 1). Recently, Ratcliffe et al. (2014) used a group of 37 Honduran police commanders to revise the organized crime Sleipnir tool for the Honduran context as part of a broader Intelligence-Led Policing training initiative. That study validated the Sleipnir approach, as well as an expert-driven process to revise it, finding “that strategic thinking tools, such as Sleipnir, can help police officers articulate specific threats to gang interdiction efforts, an important component of risk management in an intelligence-led policing environment.” (p. 2).

These experiences demonstrate the validity of using expert opinion as a viable method for developing intelligence constructs.

Intelligence Analytical Methods

The security intelligence and law enforcement communities use a number of quantitative and qualitative analytical tools, techniques and methods, including structured analytical methods, to assist in threat and issue assessment. In addition to

promoting consistency, these tools, techniques and methods enhance the quality, validity, and reliability of the intelligence product. Cope (2004) argues “while analysis certainly demands innovation and creativity ... the analytical process needs to be consistent and rigorous to ensure the patterns identified are not spurious but reliable” (p. 199).

Project Sleipnir: Background

The Sleipnir threat measurement technique was developed by Royal Canadian Mounted Police (RCMP) Intelligence Analyst Steven Strang. The technique is now used by a number of law enforcement agencies world-wide, including Canada, the United States, and some countries in both Europe and Australia.

The Sleipnir threat measurement technique “allows strategic intelligence analysts to rank-order groups of organized criminals in an objective, comprehensive and systematic way, using a consensus of expert experience and judgment as their guide” (Royal Canadian Mounted Police, 2000). Strang also developed a matrix for use with criminal extremist groups. The tool allows analysts and law enforcement agencies to improve their “understanding of the relative capabilities, limitations and vulnerabilities of organized crime” (Strang S. J., 2005, p. 2) and terrorist groups.

The alpha version Long Matrix for Criminal Extremism/Terrorism was developed by Strang in 1994. The alpha version tested the concept of structured qualitative comparison. In 1995, Strang used small Delphi surveys to develop the beta version of the Matrices. The Delphi surveys were used to increase the validity of the qualitative

comparisons. In 1998-99, Strang further developed the technique through the use of a national Delphi survey. Further refinements to the technique have been done since.

Project Sleipnir: Concepts

For purposes of discussion, the underlying concepts of the Sleipnir Long Matrix for Organized Crime will be used. The short matrix and the Criminal Extremism matrix use the same underlying principles, although the numbers, qualities, and specific attributes differ.

Sleipnir codifies organized crime into a collection of 19 measurable attributes, representing the “most important shared, observable qualities” (Strang S. , 2005, p. 2).

There are limitations to the technique:

- Reliability and validity depend on the analysts correctly “using the weights, definitions, and values”, and
- Validity depends “on the completeness and accuracy of the information used by the analysts”. (p. 2).

Project Sleipnir: Attributes

The Sleipnir long matrix for organized crime uses 19 rank-ordered attributes:

1. Corruption
2. Violence
3. Infiltration
4. Expertise
5. Sophistication
6. Subversion
7. Strategy
8. Discipline
9. Insulation
10. Intelligence Use

- 11. Multiple Enterprises
- 12. Mobility
- 13. Stability
- 14. Scope
- 15. Monopoly
- 16. Group Cohesiveness
- 17. Continuity
- 18. Links to Other Organized Crime Groups
- 19. Links to Criminal Extremist Groups

Each attribute is defined to ensure analytic consistency. For example, Corruption is defined as:

The continual efforts to corrupt public figures, representatives of the justice system and business leaders through the practices of illicit influence, exploitation of weakness and blackmail. Also the ability to place organized criminals into sensitive positions. (Royal Canadian Mounted Police, 2000, p. 28)

Additionally, each attribute has five possible values: High, Medium, Low, Nil, or Unknown. Each value is defined per attribute. This results in indicators that can be used to measure and compare groups. Sleipnir's indicators of the Corruption indicator are:

High: demonstrated ability to corrupt members of or infiltrate police forces, security forces, governments or businesses, and acquire valuable information or assistance.

Medium: some ability to infiltrate or corrupt police, security forces, public officials or business leaders, and acquiring occasional useful information or assistance.

Low: Little interest or ability to corrupt or infiltrate.

Nil: No known interest or ability to corrupt or infiltrate. (Royal Canadian Mounted Police, 2000, p. 28)

The matrix places the attributes to be measured down the vertical axis, and the groups to be compared across the horizontal axis.

Strang (2005) developed a means of assigning numerical values to each value of every attribute. By applying these values to the assessed attribute, groups can be assigned an overall numerical value, and then be rank-ordered in comparison to each other.

Thus, the Sleipnir technique provides a systematic means of conducting intelligence assessments, which in turn feed into the operational decision-making process of senior police executives.

Assumptions

This study does not address the broader issue of the vulnerability of computer systems to malicious attacks. It assumes that vulnerable systems exist and are available to capable actors.

CHAPTER TWO

RELATED LITERATURE

The late-20th and early-21st centuries have seen a phenomenal growth in society's use of information technology. This is particularly true in the West, where computerization and the Information Age have a fundamental role in almost every aspect of daily life. Individuals, industry, and government are continually adopting new and emerging technologies, integrating them into existing information technology infrastructures. On the positive side, information technologies enhance our productivity, increase efficiency, and facilitate timely communication that previously may have taken extended periods of time at great cost.

Criminals, including terrorists and terrorist organizations, have also adopted information technologies. Information technologies are used to enhance the efficiency, productivity, and effectiveness of terrorist activities and offenses. Thus, terrorists may:

- Make appropriate use of a technology to *enable* their activities (i.e. use a technology in the manner for which it was intended, although in support of terrorist activities);
- *Exploit* a technology in *support* of their activities (i.e. use a technology in a manner for which it was not intended in order to enable or facilitate their activities);
- *Exploit* a technology in a malicious manner, using it to target their victims; or
- *Damage* or *destroy* their victim's technology.

For example, in a 2012 speech at the RSA Cyber Security Conference, the FBI Director stated "Terrorists are increasingly cyber savvy. Much like every other multi-

national organization, they are using the Internet to grow their business and to connect with like-minded individuals” (Mueller, 2012) and gave three concrete examples of terrorist use of the Internet to enable their activities:

- Al Qaeda in the Arabian Peninsula has produced a full-color, English-language online magazine. They are not only sharing ideas, they are soliciting information and inviting recruits to join al Qaeda. (p. 1)
- Al Shabaab—the al Qaeda affiliate in Somalia—has its own Twitter account. Al Shabaab uses it to taunt its enemies—in English—and to encourage terrorist activity. (p. 1)
- The individuals who planned the attempted Times Square bombing in May 2010 used public web cameras for reconnaissance. They used file-sharing sites to share sensitive operational details. They deployed remote conferencing software to communicate. They used a proxy server to avoid being tracked by an IP address. And they claimed responsibility for the attempted attack—on YouTube. (p. 1)

Investigating terrorist use of information technologies generates a number of challenges for law enforcement officials. While some of the challenges are encountered during conventional criminal investigations, terrorist investigations also present unique challenges. This is particularly the case because law enforcement counter-terrorism operations include preventing, detecting, deterring, and disrupting terrorist operations, in addition to traditional criminal law enforcement.

Unfortunately, the challenges encountered during law enforcement investigations of terrorist use of information organizations are not well documented, and in some

cases are poorly understood, even among terrorist investigators. Among the challenges encountered during law enforcement investigations of terrorist use of information technology is the lack of a qualitative analytical method for assessing the cyber threat posed by terrorists and terrorist organizations.

Terrorist Use of Information Technology

Limited authoritative literature exists on the topic of terrorist use of information technologies. Presumably one of the reasons for this lack of literature is related to national security and national interest concerns and the resulting sensitivity of the information. Identifying how terrorists make use of information technology can, in some instances, serve to identify the potential challenges faced by investigators. For example, encryption and other secure communication methods present law enforcement with technical challenges related to decryption and interception (United Kingdom Cabinet Office, Performance and Innovation Unit, 1999).

We do know that information technologies are used to enhance the efficiency, productivity, and effectiveness of terrorist activities and offenses. As outlined in Table 2.1, there are four modes of potential information technology use by terrorists incidental (supportive), tactical operations, adjunct to conventional operations, and target of attack (operations).

Table 2.1 Modes of Information Technology Use by Terrorists

| Mode of Use | Explanation |
|------------------------------------|---|
| Incidental use (supportive) | Characterized by using the technology as a tool in support of terrorism offenses. For example: conducting intelligence/information gathering online; using computers to produce recruiting, training and fundraising materials; using the Internet to recruit, train, and fundraise; and communication. |
| Tactical operations | Characterized by using the technology in support of terrorist activities (operations). For example: planning (research and selection of method/target, mapping, engineering modeling, plume modeling; creating organization charts and documenting operational plans); operational communications (such as giving “go” signals and communicating during tactical operations); and targeting (selection; reconnaissance; vulnerability and risk assessments). |
| Adjunct to conventional operations | Characterized by using information technology as a medium/method of gaining access to a physical target in order to disrupt, destroy, or deny legitimate access and/or control, particularly in conjunction with a conventional “physical world” terrorist attack, perhaps (but not limited to) against a critical infrastructure target. May also serve as a distraction or force multiplier for conventional “physical world” attacks. |
| Target of attack (operations) | Characterized by information technology being the target of the attack. Although traditionally thought of as computer-based technology being the means through which to attack an information technology target, this mode of use could also include conventional “physical world” attacks where the ultimate target is an information technology system(s). Examples of this mode of use include: unauthorized access to and manipulation or deletion of data, Denial of Service (DoS) attacks; the use of malicious computer code (such as viruses, trojans, and worms), and website defacements. |

Terrorists may make use of any or all of these four modes. In addition, their use of information technology may change over time: previously used technologies may cease to be used, and new technologies may be adopted. In some cases, terrorists may revert to not using information technologies for some aspects of their activities, where such technologies had been used in the past. For example, it has been widely

reported that Osama Bin Laden stopped using satellite phones after media reports surfaced that the US government was intercepting his phone calls.

The United States Institute of Peace (Weimann, 2004) conducted a comprehensive review of terrorist-related websites and Internet activity in order to identify how terrorists are making use of the Internet. They identified eight ways in which terrorists use the Internet: psychological warfare, publicity and propaganda, data mining, fundraising, recruitment and mobilization, networking, sharing information, and planning and coordination.

In testimony before a Canadian Senate Committee reviewing the *Anti-terrorism Act*, Canadian Security Intelligence Service (CSIS) Director Jim Judd stated that al-Qaeda uses the Internet for a number of wide-ranging functions, including fundraising through credit-card fraud, recruiting, publishing training manuals, propaganda, and publicity of activities (CBC News, 2005).

The Technical Analysis Group of Dartmouth College's Institute for Security Technology Studies (2004) conducted an examination of the cyber capabilities of Islamic terrorist groups. The report's authors identified "five areas where there is clear, factual evidence that Islamic terrorism" is making use of information technologies:

1. Propaganda
2. Recruitment & Training
3. Fundraising
4. Communications
5. Targeting

In their commentary, the authors also indirectly identify a number of potential challenges for investigators, including: frequent relocation of websites, websites in Arabic-only, websites whose Arabic and English content differ substantially, the availability of training materials providing instruction on “encryption and avoiding detection while sending electronic communications” (p. 18), the provision of specialized training in overt and covert cyber attack methodologies, the recruitment and participation of highly technically-skilled terrorists, and pro-jihadi Web forums providing advice on “online security, encryption, steganography, proxies and anonymizers, and IDS” (p. 37).

Adoption of Information Technology

The successful adoption of any information technology generally requires the user to go through a series of steps, from researching the technology, to experimenting and training with it, then to implementing its use. For example, when considering terrorist use of new technology, including information technology, one possible model might includes these five distinct stages of technology adoption:

- Interest
- Acquisition
- Experimentation and/or training
- Use (terrorist or non-terrorist activities-related)
- Offensive use (terrorist activities)

Not all terrorists and terrorist organizations will clearly move through all stages. Nor will all technologies be successfully implemented. Technologies, terrorists, and terrorist organizations may stop at any stage for any technology. A lack of available information may result in an inability to identify the stage a terrorist's use of any given information technology, or information technology in general, is at.

Until the early part of this century, little academic examination of terrorist innovation was conducted, despite over two decades of the study of technological innovation. Prior to this, innovation researchers, particularly those exploring technological innovation and/or contagion, dissemination or diffusion of innovation – from Midlarsky, Crenshaw and Yoshida (1980), Rogers (1982), Bonneuil and Auriat (2000), Bloom (2005), Dugan, LaFree and Piquero (2005), to Braithwait and Li (2007) – were limited to individuals and traditional organizations, such as corporations. Examination of terrorist innovation did not begin until around 2005, and remains very limited: the primary works are Jackson et al (2005), Dolnik (2007), Rassmussen and Hafex (2010), and Gill, Horgan, Hunter and Cushenbery (2013).

As late as 2010, Rassmussen and Hafex argued “innovation is a constant feature of terrorism, yet little is known about how terrorists innovate, the factors that drive them to innovate, and the indicators that could help predict their trajectory toward innovation” (p. 2). In this context, Rassmussen and Hafex hosted a workshop which invited experts and researchers to examine innovations among terrorist groups, particularly in relation to innovation preconditions, causes, and predictive indicators. With the support of illustrative case studies, the experts reached several consensus conclusions regarding preconditions and causes, including:

- Terrorist innovation is often a product of a gradual, incremental synthesis of earlier innovations, rather than a dramatic leap in terrorist tactics and technologies.
- Terrorist innovation is usually motivated by problem solving intended to overcome constraints in the security environment, or limitations in the political one. Terrorists seek new technologies, targets, or opportunities in order to circumvent security measures, revitalize support for their cause, pursue a new strategy to remedy failed ones, or simply escalate a conflict because lower levels of violence are assessed to be ineffective.
- The important role of ideology or “toxic grievances” in inspiring and legitimating WME [Weapons of Mass Effect] attacks, especially the ones that concern mass destruction and mass casualties among civilians. Groups with grandiose worldviews, millenarian ideologies, or deep feelings of humiliation are less likely to impede the use of mass casualty terrorism than those with clearly defined objectives. (p. 2-3)

The same workshop also examined predictive indicators, “the observable steps and preparatory behaviors leading to the innovative terrorist attack and that could have revealed the terrorists’ intent had they been investigated thoroughly” (p. 4). The experts found that “predictive indicators are not universal; any potential list of indicators must be confined to the specific innovation sought after by the terrorists. This finding suggests that security specialists may have to proceed on a case-by-case basis when seeking to anticipate and foil deadly innovations” (p. 4). This directly supports the approach taken in this study: identify a series of indicators of intent and capability which can be used to

assess the level of cyber threat posed by terrorist organizations and individuals – a functional construct confined to a specific innovation (the ability to conduct cyber attacks). Further, Rassmussen and Hafex model of using expert opinion to inform an issue is also appropriate for the problem examined by the current study.

Finally, the workshop's participants identified some specific predictive indicators to consider, including:

- Specific threats made in terrorist leaders' statements are one predictive indicator of innovation commonly found in the cases analyzed in this workshop. Another salient indicator is prior attempts by the terrorist group to deploy innovative tactics.
- Earlier failures in terrorist innovation should not be taken lightly because they could serve as indicators of future intent as well as opportunities for the terrorists to experiment and learn through trial and error. Underestimating the terrorist adversary and the failure of the authorities to investigate with due diligence its prior activities often precedes successful WME attacks.

Threat Posed by Terrorists and Terrorist Organizations

In 2001, Canada's Office of Critical Infrastructure Protection and Emergency Preparedness released a *Threat Analysis of Al-Qaida's Cyber Capability*, identifying five key judgements:

- Al-Qaida (the group formed and led by Osama bin Laden) has not engaged in computer-based attacks in the past. However, in the wake of the World Trade

Center (WTC) attacks, bin Laden has suggested that Al-Qaida has the expertise to use the computer as a weapon.

- Given the economic damage the United States suffered due to the WTC attacks, it is possible that those responsible may shift their sights away from primarily symbolic targets, such as heavily populated buildings or sports stadiums, toward critical infrastructures.
- Bin Laden's base for his operations, Afghanistan, does not provide an ideal venue for staging cyber attacks.
- A potential cyber terrorist attack by the Al-Qaida group, or its sympathizers, would likely be launched or coordinated outside Afghanistan.
- Retaliatory cyber attacks – primarily web defacements – from individual sympathetic hackers on both sides have commenced and will continue to occur.

(p. 1)

Unfortunately, there is little authoritative public literature about the cyber threat posed by terrorists and terrorist organizations. There remains considerable speculation among the press and other sources about the threat terrorists may pose. This speculation ranges from “no threat” to a significant threat on the level of an “electronic Pearl Harbor”. The lack of concrete information may in part be due to the fact that there are no confirmed instances of terrorists conducting cyber attacks (Brickey, 2012). The closest are perhaps examples of distributed denial of service attacks or web defacements during times of political conflict (Clarke & Knake, 2010).

Threat Assessments

A number of models for conducting threat assessments are in use within the security and intelligence community. None specifically address cyber threats, particularly those posed by terrorists and terrorist organizations.

Terrorist threats are asymmetric threats. That is, they involve the element of surprise and are thought of as “not playing fair”. The threat posed by terrorists is magnified because their attacks tend to target civilians who lack defensive measures.

Threat assessments are a product of threat analysis. They provide a basis for risk assessments and are a tool for countermeasures and operations planning. Threat assessments identify the threat, intentions, capability, and probability. Threat assessments are part of the intelligence process, supporting threat warning and risk management decisions. Threat assessments drive operational planning.

Preparing a threat assessment is a multi-step process. *Threat analysis* involves the collection of all-source information that will be used in determining threat levels. It forms the basis for creating the threat assessment. *Defining the current threat level* requires the establishment of benchmarks for judging an increase or decrease in threat activity, and for defining the degree of threat. The *threat assessment* itself identifies and assesses the threat, intent, capability and probability.

Threat assessment methodologies developed for related purposes (such as physical terrorist threats) have components which can be adopted for use in assessing cyber threats.

Threat analysis typically examines three categories: capabilities, intentions and probability, exploring representative elements of each. Table 2.2 outlines these three

categories when examining physical terrorist threats, and provides a small number of examples of their sub-elements.

Table 2.2 - Physical Threat Analysis Methodology

| Category | Elements |
|---|--|
| Capability <i>the acquired, assessed, or demonstrated level of capability to carry out the threat</i> | <ul style="list-style-type: none"> • Mass casualty capability • Targeting • Access to weapons/weapon materials • Method of operation • <i>Different tactics may = different threats</i> |
| Intentions <i>whether the individual/group or organization has the intent to carry out the defined threat, including their stated desire and/or actual history of carrying out threats against target</i> | <ul style="list-style-type: none"> • Recent attacks • Willingness to conduct attacks • Ideology • Attacking similar targets elsewhere • Stated intentions |
| Probability: Activity <i>probability is the likelihood of the threat being perpetrated by an individual/group or organization. Prob = f(capability x intention)</i> | <ul style="list-style-type: none"> • Disruptions by government authorities • Operational & support activity • Credible indications of targeting • Operational tempo |
| Probability: Operating environment <i>how the overall environment influences an individual/group/organization's ability and motivation to conduct an attack</i> | <ul style="list-style-type: none"> • Police and Security presence • Security measures • External influencing factors |

Threat levels are then assessed in terms of activities, capability, and intent. For example, the United Kingdom's security intelligence community uses the following seven threat levels with respect to terrorism (Intelligence and Security Committee (UK), 2006, pp. 18-19):

NEGLIGIBLE (Level 6) – available intelligence and recent events indicate that terrorists currently have no capability and/or no intent to mount an attack on the target. It is assessed that an attack is very unlikely to be mounted.

LOW (Level 5) – available intelligence and recent events indicate that terrorists currently have little capability and/or intent to mount an attack on the target. It is assessed that, although it cannot be ruled out, an attack is unlikely to be mounted.

MODERATE (Level 4) – available intelligence and recent events indicate that terrorists currently have some capability to mount an attack on the target and such an attack would be consistent with the group's general intent; or that they have the capability but their intent is qualified by current circumstances. It is assessed that an attack is possible.

SUBSTANTIAL (Level 3) – available intelligence and recent events indicate that terrorists have the capability to mount an attack on the target and that such an attack is within the group’s current intent. It is assessed that an attack is likely to be a priority for the terrorists and might well be mounted.

SEVERE (GENERAL) (Level 2(G)) – available intelligence and recent events indicate that terrorists have an established capability and current intent to mount an attack on the target or targets of this nature. It is assessed that an attack is a priority for the terrorists and is likely to be mounted.

SEVERE (DEFINED) (Level 2(D)) – available intelligence and recent events indicate that terrorists have an established capability and current intent to mount an attack on the target and there is some additional information on the nature of the threat. It is assessed that an attack on the target is a priority for the terrorists and is likely to be mounted.

CRITICAL (Level 1) – available intelligence and recent events indicate that terrorists with an established capability are actively planning to attack the target within a matter of days (up to two weeks). An attack is expected imminently.

Threat and risk matrices may aid in the decision process for assessing the current threat level. A threat matrix considers what is known about the threat parameters (identity, capability, hostile intent, and probability) and provides a matrix for assessing the threat level. Matrices use defined category levels, which are in concept very similar to the UK’s threat levels detailed above.

In developing its Consolidated Risk Assessment (CRA) examining over 50 scenarios, for example, the Government of Canada’s Chemical, Biological, Radiological Nuclear (CBRN) Research and Technology Initiative (CRTI) uses two matrixes: risk matrix, and preparedness prioritization matrix. The CRTI CRA risk matrix, a copy of which is provided in Table 4.3, combines risk rating scales related to technical feasibility (of a scenario) and impact (DRDC CRTI, 2005). Impact components considered

include: potential number of dead or injured, damage to equipment, buildings, or the environment, and economic loss.

Table 2.3 CRTI's CRA Risk Matrix Table

| RISK MATRIX | | | | |
|--------------|--------------------------------|----------|----------|----------|
| IMPACT | RELATIVE TECHNICAL FEASIBILITY | | | |
| | HIGH | MEDIUM | LOW | VERY LOW |
| CATASTROPHIC | Extreme | Extreme | High | Moderate |
| CRITICAL | Extreme | High | High | Low |
| MODERATE | High | Moderate | Moderate | Low |
| LOW | Moderate | Low | Low | Low |

CRTI's Preparedness Prioritization Matrix, a copy of which is provided in Table 2.4, combines Risk with Intelligence Judgments about the likelihood of a scenario (DRDC CRTI, 2005):

Table 2.4 CRTI's CRA Preparedness Prioritization Matrix

| PREPAREDNESS PRIORITIZATION MATRIX | | | | |
|------------------------------------|-----------------------|------------------|------------------|------------------|
| RISK | INTELLIGENCE JUDGMENT | | | |
| | LIKELY | EMERGING | POSSIBLE | UNLIKELY |
| EXTREME | Immediate | Immediate | High | Emerging Concern |
| HIGH | Immediate | High | High | Discretionary |
| MODERATE | High | Emerging Concern | Emerging Concern | Discretionary |
| LOW | Emerging Concern | Discretionary | Discretionary | Discretionary |

While the CRTI CRA matrices are used to produce an investment framework for identifying areas for scientific investment, the use of threat and risk matrices of various forms is a common approach for assessing threats and risks, particularly in complex environments.

Cyber Threat Posed by Terrorists and Terrorist Organizations

I conducted a search of open literature using Google and academic journal databases. I found there is no literature discussing or providing a methodology for assessing the cyber threat posed by terrorist organizations and individuals. It is expected that the lack of such a methodology limits the robustness, reliability, and consistency with which terrorist cyber threats are assessed.

Indicators of Terrorist Behavior

To develop a functional construct using indicators of intent and capability, it is useful to gain insight into terrorist behaviour in general. For example, Chatagnier, Mintz and Samban wrote extensively on terrorist group decision-making (2012). They note that “leaders of terrorist organizations make the critical decisions” and the leaders “drive the organization’s decisions and actions” (p. 125), although they also found that the structure of a terrorist organization has influence on the pattern of decision-making by organization leaders.

A review of media reports, press releases and government reports on conventional terrorists and their activities (such as media reports of terrorist arrests, trials, and convictions), identified a number of areas for consideration to turn into indicators of intent and capability suitable for this study. These include:

- The influence terrorist group leaders have on decision-making (for example, some groups are very hierarchical with rigid decision-making practices, while a lone actor may be the sole decision-maker).
- A history of past activity and what that activity was.

- Whether the group's past history indicates an evolution or innovation in tactics and methods, or whether they use the same time-tested methods again and again.
- Public statements of intent to carry out certain acts (which may or may not correlate to actual plans).
- Plans to carry out certain acts, and how well-developed those plans are.
- Prior foiled plans, unsuccessful attempts, and successful attacks (most of the cases reported in the media involve foiled plans, where government authorities have intervened before an attack was carried out, usually through arrests and prosecution through the courts).
- Whether there are ideological underpinnings for the types of attacks the group carries out or the methods they use.
- Whether the written literature of the group, in the form of doctrine, training material, and propaganda, supports (or, conversely, does not support) the use of specific types of attacks and/or methods.
- How much harm the group wishes to cause. For example, a group may be willing to conduct bombings, but they will always call in a warning first to minimize the cost to human life. Another group may only target military and government targets and be unwilling to target civilians.
- Whether the group has a policy regarding how they will use cyber methods. For example, a nation may have nuclear weapons, but their policy is that they will not use them as a first-strike weapon, only defensively.

- The nature and extent of specialist expertise and resources group members have. For example, a terrorist group may have a master bomb-maker amongst their personnel.
- The nature and extent of specialist expertise and resources a group has access to from others. For example, a group may not have expertise in bomb-making, so they acquire that expertise from another group with whom they are allies.
- The nature and extent of necessary materiel a group has access to. For example, if a group wanted to post propaganda videos on the internet, they would need access to a video camera, the ability to record digital video (or convert conventional video to digital video), a website or web service on which to upload the video (which may require an account at the service), and internet access to do the uploading. They may also want to make use of video editing and other resources to improve the quality and professionalism of their video.
- Whether the group has the ability to infiltrate target organizations to gain information or launch an attack.

Because several of these indicators are indicators of intent and several are indicators of capability, grouping them into those respective groups for the purposes of the construct would make it less confusing for analysts to use. It would also make it easier to develop an overall assessment of intent and an overall assessment of capability, as each could be measured separately with a small and manageable number of indicators – a process that could be done manually without quantitative metrics behind-the-scenes.

CHAPTER THREE

METHODS

Introduction

The purpose of this study was to leverage the professional subject matter expertise of a group of government employees to develop a new construct – a structured analytical tool instrument to assist intelligence analysts and researchers in the assessment of the cyber threat posed by terrorist individuals and organizations. I believe the creation of such an instrument, where one is currently lacking, will support analytical work in this area, eventually becoming an additional tool in the analytical methodology toolbox that analysts and researchers may apply to the assessment problem. The primary purpose of developing a structured analytical tool is to increase the consistency, validity, and reliability of assessments, individually, across time, and when comparing groups amongst each other.

The overarching question of this research was what would such an instrument look like? With participants being provided an initial prototype analytical tool instrument, the research questions for the participants revolved around what the structure and content (explanatory material, indicators) of the final construct consensus instrument should look like as it evolved from the prototype. The study also sought to validate the final instrument to some degree through the assessment of fictional vignettes by the study participants.

The purpose of this chapter is to describe the methodological approach undertaken for this study. The chapter includes discussions of issues related to the methodological approach, including (a) who were the research participants,

(b) summary of information needed to conduct the study, (c) a description of the research design, (d) creation of the prototype analytical tool instrument, (e) data collection methods, (f) data analysis methods, (g) ethical considerations, (h) issues of trustworthiness, and (i) limitations of the study, followed by a concluding summary.

Research Participants

A purposeful sampling procedure was used to select appropriate participants for this study. As the study draws on knowledge from multiple domains within the law enforcement, national security, and intelligence analysis communities, I sought to locate participants who would be able to contribute a range of professional experience.

Three participants were identified for an initial group, all of whom were professionally known to me. These participants would ultimately become the participants in Group One (G1), as discussed later. In order to identify additional participants, a snowball sampling strategy was used, whereby potential participants were asked to refer other individuals who they believed were suitable subjects given the participant criteria. The criteria for selection of participants were as follows:

- All participants were government employees.
- All participants were employees of departments, agencies or organizations that have a law enforcement, national security, criminal intelligence, national defense, and/or critical infrastructure protection mandate.
- All participants had extensive professional experience in the fields of intelligence analysis/research, national security investigations, cyber threat investigations or analysis, and/or intelligence analysis methodology development.

- Although extensive professional experience was not specifically defined, it was expected. the participants would have understood it to mean a minimum of three to five years experience.

This snowball sampling allowed for the identification of additional prospective participants beyond those who were originally identified. The total pool of prospective participants identified included 12 individuals, of whom nine agreed and were available to participate in the study. Three of these nine participants were unable to participate in the focus group because external circumstances unrelated to the study prevented their attendance at the focus group on the day it was scheduled to occur. Thus, six subjects participated in the focus group. Because the study used an iterative process, the input these participants provided in the phases prior to the focus group was included in the study.

Participant Demographics

Although participants were all experienced government employees, there was variation in their current and past job positions, the duration of work experience in those positions, and the extent of experience in identified domain areas.

Current job positions held by participants include: intelligence analyst/researcher, manager of intelligence analysts/researchers, manager of policy analysts, security management, researcher, and security analyst. Although all participants were government employees, they worked for different types of organizations: four with law enforcement organizations, one with a defense/military organization, and three within other types of government departments/agencies/organizations. The majority of

participants had extensive experience in their current position: two had only zero to less than five years' experience, while the remaining six had five or more years' experience – four had five to less than ten years, and one each had ten to less than 15 years and one had 15 to less than 20 years. One participant was currently a peace or police officer, and one participant had previously been a peace or police officer. One participant did not complete the demographics survey.

The participants were asked about their current and previous job positions. Their positions have varied and included:

- Intelligence analyst/researcher
- Manager of intelligence analysts/researchers
- Intelligence officer
- Other law enforcement
- Other law enforcement (manager)
- Policy analyst
- Manager of policy analysts
- Security management
- Researcher
- Intelligence special advisor
- Signals intelligence gathering and analysis
- Military officer
- Academic
- Scientist
- Computer analyst

The majority (six) of participants were currently or previously had been intelligence analysts/researchers.

Participants were asked how many total years of experience they had working in a list of specific areas. In addition to one participant making two choices for two areas (denoted with a * in Table 3.6), one limitation of the survey question was that it did not include a “zero” option, but rather it began with zero to five years. While most participants only checked the years of experience they did have, leaving the other areas with no marking, others checked years of experience for all areas, with many areas marked zero to five years. It was not possible to determine for those participants if the zero to five represented zero experience or experience of greater than zero to less than five years. Understanding the existence of this issue, as noted in Table 3.6, all participants had some national security experience, with most having experience in criminal investigations and criminal intelligence. The area in which participants had the least experience was cyber crime investigations, although many had experience in cyber crime intelligence. Some participants had at least fifteen years of experience in national security, criminal investigations, criminal intelligence, and security management. Several participants had five or more years of experience in analytical or other methodology research.

Finally, all participants had at least five to ten total years of experience working in any combination of the areas specified in Table 3.6. The overall work experience in the specified areas ranged from five to 30-to-35 years (Table 3.5).

Table 3.5 Combined Total Years of Experience in Specified Areas of Work

| | Total years of experience (number of participants) | | | | | | | | |
|---------------------------|---|------|-------|-------|-------|-------|-------|-------|-------|
| | 0-5 | 5-10 | 10-15 | 15-20 | 20-25 | 25-30 | 30-35 | 35-40 | 40-45 |
| Total combined experience | | 1 | 1 | 2 | 2 | 1 | 1 | | |

Table 3.65 Total Years of Experience per Specific Relevant Areas of Work

| Specified area | Years of experience (number of participants) (multiple areas of experience may be concurrent) | | | | | | | | | |
|--|---|-----|------|-------|-------|-------|-------|-------|-------|-------|
| | No selection | 0-5 | 5-10 | 10-15 | 15-20 | 20-25 | 25-30 | 30-35 | 35-40 | 40-45 |
| National security | | 2 | 3 | 1 | | 2 | | | | |
| Security intelligence* | 2 | 5 | 2 | | | | | | | |
| Criminal investigations | 3 | 1 | 1 | 1 | | 1 | 1 | | | |
| Criminal Intelligence | 1 | 2 | 1 | 1 | | 2 | 1 | | | |
| Cyber crime investigations* | 4 | 4 | | 1 | | | | | | |
| Cyber crime intelligence | 2 | 5 | | 1 | | | | | | |
| Critical infrastructure protection | 2 | 4 | 1 | 1 | | | | | | |
| Emergency management | 4 | 2 | 2 | | | | | | | |
| Security management | 2 | 4 | 1 | | | 1 | | | | |
| Analytical methodology research | 2 | 2 | 1 | 2 | 1 | | | | | |
| Other methodology research | 3 | 2 | 1 | 2 | | | | | | |
| Data provided for the returned questionnaires. Two items (*) add to more than the questionnaire total owing to multiple selections being made by the participants. | | | | | | | | | | |

Information Needed to Conduct the Study

This study leveraged the professional experience of nine government employees to develop a new construct – a structured analytical tool designed to assess the cyber threat posed by terrorist individuals and organizations. Fundamentally, participants

answered the research questions of: how such an analytical tool should appear, what it should contain, and how it should function.

Overview of Research Design

This study used a multi-phasic approach in order to approximate an IEG process. The following is a summary of the steps taken to undertake this research. A more detailed explanation of the steps is provided in the subsequent sections.

1. Following the proposal acceptance, a review of relevant open source literature was conducted. This included publically accessible government publications and reports, academic studies and publications, books, and media reports. Synthesizing the totality of the information reviewed, a prototype analytical tool instrument was produced (Appendix A).
2. University of North Texas Institutional Review Board (UNT IRB) approval was received to conduct this study. Informed consent, both oral and written, was obtained from all participants.
3. Participants were divided into two groups: group one (G1) had three participants and the remaining six participants comprised group two (G2).
4. All participants were emailed a demographics questionnaire. The questionnaire was designed to collect information about the participants' current job as well as current and past work experience, particularly as related to specified areas of work.
5. G1 participants were emailed the prototype analytical tool instrument and a prototype analytical tool questionnaire. After a period to review the prototype

analytical tool instrument, participants were individually interviewed in person to discuss their responses to the analytical tool questionnaire. The participants also provided written answers to the questionnaire. The purpose of the questionnaire was to learn the opinion of each participant regarding:

- a. If and how the structure of the instrument should be revised.
 - b. If and how the indicators used in the instrument should be revised.
 - c. If there were any other changes that should be made to the instrument.
6. Information collected from the written feedback and interviews was collated and used to rework the prototype analytical tool to create a revised analytical tool instrument (Appendix B).
7. G1 and G2 participants were emailed the revised analytical tool instrument and a revised analytical tool questionnaire (which asked the same three questions as the prototype analytical tool questionnaire). Participants emailed back their responses to the questionnaire.
8. Two summary documents were produced using the feedback provided by the participants. The first document was a list of general comments provided by the participants pertaining to changes to the structure, changes to the definitions, and other recommended changes to the instrument. The second document contained specifically recommended changes to the indicators in the instrument. These documents were provided to groups G1 and G2 participants by email prior to the focus group.
9. A day-long (eight hour) focus group was held consisting of the combined group of G1 and G2 participants. The overall purpose of this focus group was two-fold:

(a) to rework the revised analytical tool until a consensus was reached on its appearance and its specific contents, and (b) to conduct an initial validation of the final version of the tool utilizing hypothetical vignettes (Appendix D) and an opinion questionnaire.

Prototype Analytical Tool Instrument Creation

I conducted a review of the relevant open source literature, including publically-accessible government publications and reports, academic studies and publications, books, and media reports. The purpose of this review was to gain insight into an appropriate structure and possible indicators for the instrument. Synthesizing the totality of the information reviewed, I produced a prototype analytical tool instrument (Appendix A). Some primary conclusions drawn from this synthesis, which informed the structure were:

- The need for detailed instructions on the purpose of and how to use the instrument.
- The need to separate the two components of threat, intent and capability, into separate groupings to be then measured independently of each other, and whose overall outcomes are then combined to inform the level of threat. This approach is indicated, for example, in the language of the United Kingdom's security intelligence community's terrorism threat levels (Intelligence and Security Committee (UK), 2006) and the Government of Canada's CRTI CRA matrices (DRDC CRTI, 2005).

The decision to separate indicators into two tiers, tier one and tier two, was an innovation I devised as a solution to the challenge of some indicators appearing to be of greater importance or carry more weight than others, yet still maintaining the instrument as qualitative in nature and not quantitative. This use of tiers allowed for some degree of weighting without requiring quantification.

IRB Approval

Approval to conduct this study was obtained from the University of North Texas' (UNT) Institutional Review Board (IRB) in June 2014. Oral and written informed consent, using an informed consent form approved by UNT's IRB, was obtained from all participants.

Data Collection Methods

The study used multiple methods of data collection within an iterative process in an attempt to approximate an IEG process. The methods employed by this study included questionnaires, interviews, and a focus group.

Phase One: Revision of the Prototype Analytical Tool Instrument

The three G1 participants were emailed a copy of the prototype analytical tool instrument as well as a questionnaire about the instrument's revision. The questionnaire did not collect personal information about the participants. In addition, participants were informed that their responses may be anonymously shared with other study participants and/or quoted in this dissertation or other works based on the study.

Therefore, they were advised that all responses must only include unclassified material or information.

The questionnaire asked three questions based on each participant's area of expertise, professional experience, and opinion:

1. What changes, if any, would they make to the STRUCTURE of the Tool?
2. What changes, if any, would you make to the DEFINITIONS used in the Tool?
3. What, if any, OTHER CHANGES would you make to the Tool?

Each G1 participant provided their responses to the questionnaire in two forms: firstly, by comments accompanying or on the prototype instrument, and secondly, through an in-person interview discussion of their responses conducted by myself. The interview discussion allowed me to develop a more complete understanding of their responses, including nuances which could not be conveyed effectively effectively in writing. Additionally, it exposed further issues that had not been previously addressed in their written responses, which further informed the revision process.

I correlated, assessed, and synthesized the participants' responses in order to rework the prototype analytical tool instrument, creating the revised analytical tool instrument.

Phase Two: Reworking of the Revised Analytical Tool Instrument

For the remainder of the study, G1 and G2 participants were merged into one functional group comprising all of the study participants. The participants were emailed the revised analytical tool instrument and another copy of the same analytical tool

questionnaire previously used. In this phase, all responses were provided via email, using a combination of narrative responses and mark-up of the instrument text.

I collected all of the narrative responses into a single document, with individual responses stripped of all identifying information to protect the participants. Simple revisions to the indicators I collected into a second document which included only those indicators where a participant(s) had recommended changes, and the nature of those recommended changes. These two documents were provided to participants by email prior to the start of the focus group.

Phase Three: Focus Group

Of the nine original participants, only six were able to participate in the one day, eight-hour focus group. The other three had to decline participation in the focus group due to external circumstances making them unavailable on the day the focus group took place.

At the beginning of the day, after the completion of administrative formalities, the participants were provided with a document containing five hypothetical vignettes (Appendix C), representing two fictional terrorist organizations and three fictional terrorist individuals. Unable to use real information about real terrorist groups (because that type of information inherently involved sensitive information), I created the vignettes using the types of descriptions of terrorist behavior, intentions, and capabilities found throughout media and in other public reporting. The vignettes are hypothetical, and while they may resemble real organizations, they are entirely works of fiction. The use of vignettes in both quantitative and qualitative studies is an accepted social science

practice (Barter & Renold, 1999). There are multiple ways in which vignettes are used in research. For example, Atzmüller and Steiner (2010) note “vignette studies use short descriptions of situations or persons (vignettes) that are usually shown to respondents within surveys in order to elicit their judgments about these scenarios” (p. 128), while Wason, Polonsky, and Hyman (2002) explain that “in empirical marketing studies, vignettes are increasingly used to develop measurement scales, assess public/organizational policy, and study key variables in judging the decisions or actions of a protagonist” (p. 41). In the current study, vignettes were used as a proxy for factual descriptions of real terrorist organizations and individuals to enable participants to conduct assessments of the level of cyber threat the organization or individual in each vignette represented. The vignettes were used to validate the final analytical instrument developed by participants.

The participants were asked to individually use their professional, expertise, experience, and opinion to conduct an assessment of each fictional vignette and to indicate in the provided table their assessment of the level of cyber threat each organization or individual represents to CountryA. All focus group participants read the vignettes and completed the paper assessment before the entire group moved onto the next portion of the day.

The bulk of the focus group day was spent discussing how to further modify the revised analytical tool instrument to engineer a final version that, by consensus, the participants felt was suitable and valid as a final version of the instrument. As its base, the discussion was guided by the same three questions as the analytical tool questionnaire used in the previous phases.

Once a consensus was reached on a final version, the participants returned again to the hypothetical vignettes. This time, instead of conducting an individual exercise in assessment, the entire group collectively assessed the vignettes using the new final version of the analytical tool instrument. This assessment involved discussion amongst the participants of how particular indicators should be scored and why.

After the vignettes were scored, the group was provided with a final paper questionnaire. This questionnaire examined participant perceptions about the utility and value of the analytical tool as well as structured analytical tools in general.

Data Analysis Methods

Data collection and analysis occurred sequentially in phases, as responses from one phase informed the input material for the subsequent phase.

In order to protect participant confidentiality, no data coding attributing the responses to a specific individual was conducted. Rather, responses were tallied in the aggregate or collected together so an individual response could not be tied in any way to a specific individual.

Ethical Considerations

The primary ethical consideration in this study was the protection of participant identities before, during, and after this study. Although the focus group participants became aware of the identities of the other participants through the focus group, participant identities were not shared outside the focus group participants. The identities of the three participants who were unable to participate in the focus group

were not shared with the focus group participants. There was, however, a small level of awareness of the fact that specific individuals were participating in the study: some of the participants chose to share fact of their own participation in the study with work colleagues, and some participants were required to notify and/or obtain permission from their managers to participate in the study. These were not considered breaches of confidentiality as the participant themselves was choosing to do the informing to others.

Coupled with participant confidentiality was institutional confidentiality. For this reason, the names and other potentially identifying characteristics of the government organizations to which the participants are affiliated was kept confidential.

Voluntary and informed consent was obtained from all participants. Initially this consent was obtained verbally by telephone or in person following a discussion between myself and the prospective participant of the study and the anticipated risks. Follow-up written consent was then obtained at the first in-person meeting with each participant. For G1 participants, this occurred at the start of the interview; for the remainder of the participants it occurred before or at the start of the focus group session.

The focus group operated under a modified version of Chatham House Rules: no individual or organizational attribution may be made for any of the discussion during the focus group.

To further protect participant confidentiality, measures were taken to secure the storage of study-related information. I am the only person with access to personally/individually identifiable information relating to the participants and/or the organizations for which they work.

Finally, this study was conducted at an unclassified level, including the review of literature to develop the prototype analytical tool instrument as well as interviews with participants, questionnaire responses from participants, and feedback and discussions during the focus group.

Issues of Trustworthiness

All of the subjects were professionally known to me, either directly or indirectly. This immediately established a high level of rapport between the participants and me. In addition, all of the participants professionally knew or knew of each other, which also created an immediate atmosphere of trust amongst them. Trust did not have to be developed; it inherently existed and was implied. I believe this trust enabled fulsome participation in the study within the limitation of the study being conducted in the absence of confidential/sensitive information.

Limitations of the Study

This study has a number of limitations which revolve around it being conducted at an unclassified level, the artificiality of the study context, and the small sample size.

As noted previously, this study was conducted exclusive of confidential/sensitive/classified information. This limited the breadth and depth of discussion and feedback which could occur, as some relevant feedback that would otherwise have informed the development of the tool was sensitive and thus could not be provided by participants. While this is a limitation, particularly of the focus group discussions (such as putting a limit on the ability to provide some illustrative examples),

participants were confident at the end of the focus group that they had developed a valid final version of the instrument.

The study only approximated, and did not exactly replicate, an IEG environment. According to private communication with several individuals who have participated in IEGs (2014), a normal IEG does not include participant anonymity, which was required for this study. Further, according to the same individuals, for the development of a tool such as this, there would likely be several rounds of email revisions, first within a small group (often within a single agency, prior to bringing the proposal to the wider IEG), and then amongst the members of the IEG. Email exchanges and in-person IEG discussions often intermix, and there are often multiple in-person group meetings, often interspersed by further email revision rounds, before the IEG group achieves consensus on a final product. This study, by necessity, accelerated and modified the process.

Finally, the small study size is both a benefit and a limitation. The small size made the process of collating responses and consequent modifying the instrument easier. I believe it also contributed to the positive, collegial, and collaborative environment that existed during the focus group – the size was small enough that everyone was able to comfortably contribute as they wished to. The disadvantage of the small number of participants is that the diversity of expertise contributing to revising the instrument was limited to a small number of people. For example, there was only one current peace or police amongst the participants. While I believe the participants were strong subject matter experts whose opinions were credible, reliable, and valid, a larger number of participants could have a greater breadth of insight and may have brought additional ideas for consideration.

Summary

In summary, this chapter provided a summary of the research approach used for this study. A multi-phasic, multi-method approach was used to solicit the opinions of the nine participants, all of whom were experienced government employees. The data collection methods included questionnaires, interviews, and a focus group, which leveraged participant's professional experience to develop a new construct, an analytical tool to assess the cyber threat posed by terrorist individuals and organizations.

Although the study approximated, but did not replicate, a genuine IEG, the resulting final analytical tool instrument represents the consensus agreement of the participants. It is hoped that the instrument will be of value to assist intelligence analysts and researchers in their assessments, will in turn identify potential intelligence gaps, and may inform decision makers' priority setting and thus resource allocation.

CHAPTER FOUR

RESULTS

Throughout this chapter, the construct is referred to as an analytical tool or tool, language the participants were familiar with and which was used when interacting with them in place of the terms construct or functional construct.

Revision of the Prototype Analytical Tool

The revision of the prototype analytical tool took place following individual in-person interviews with each of the three G1 participants, in conjunction with the written feedback they chose to provide. The following subsections discuss these participants' recommended changes. Due to participant confidentiality issues, the material will be presented in the aggregate and not ascribed to individual participants.

Reworking of the Revised Analytical Tool

General Discussion About the Tool

The tool is intended to be an “aid to judgement”. In this sense, the supporting narrative must discuss the unknowns, and address the intelligence gaps they represent. If there are sufficient unknowns, this aspect of the group/individual becomes an intelligence requirement. The narrative will also describe specific examples which will justify the ratings and note the level of reliability and validity of the information.

The tool has the potential to be used to compare a group's capabilities and intent against a number of specific targets, such as SCADA, databases, etc. The narrative

would have to clearly reflect the very focussed use of the tool in this manner. Some of the aspects of the tool that participants liked:

- The tool's potential for use to both assess a specific as well as for general threat assessment.
- The insistence that a supporting narrative accompany the matrix.
- The distinctions between intent and capability measures, and how that distinction is reflected in the Threat Level Table at the end.
- The practice of listing the indicators from Unknown to High.

Introduction and Instructions on How to Use the Tool

Consideration should be given to using the term “criminal extremist” in place of “terrorist organization/individual” as it is a more neutral term, since ideologically-motivated hackers may be trying to accomplish irritation, embarrassment, and incapacitation of their target, rather than terror. The decision was made to hold this decision until the focus group was able to discuss it (their decision was to change the phrase from “terrorist organizations and individuals” to “terrorist entities and individuals”).

Concerns were raised over how to define “cyber threat”. Participants felt that a definition of what is meant must to be provided, specifically, cyber as a means of attacking cyber targets. This is important to distinguish it from other uses of computers. Further, it is important to distinguish that this tool will be for examining the use of cyber as a method to attack cyber targets, as opposed to kinetic methods against physical

targets. Another definition identified as required was a definition of terrorist organization. It was noted that the definition should be tied to relevant criminal laws.

When discussing the accompanying narrative, there was discussion about the strength of information used to conduct the assessment. For example, did there need to be some way to indicate the strength of sources, or their reliability or validity? This speaks to the way the information is used by the analyst in conducting the assessment, and demonstrates the need for qualifiers and a narrative to accompany the tool, not a single tool as a stand-alone item. The issue of indicating source strength was ultimately resolved during the focus group by including such an indicator in a worksheet that accompanies the tool.

Another question was does it matter how the information is obtained? How does the analyst weigh information from one source over another if they are in conflict? Or, for example, would single source information from one agency be sufficient to do an assessment? Through discussion it was clarified that both such scenarios can use the tool, but they must be explained clearly in the narrative.

The statement “this tool can be used by an analyst alone, or a group of subject matter experts” or a variation of it, was identified as needing to be added to the step-by-step instructions on how to use the tool.

Indicators

Cyber attack history should also consider the success of attacks against other country targets, and the vulnerability of those systems. For example, were the systems well-protected or not well-protected? The measure could be along the lines of: the

degree of success: well protected, moderately protected, poorly protected, and no success. Analytical judgement comes into play numerous times with this indicator. The analyst will have to determine how to account for an attack that happened, the group that claimed responsibility for, but for which the claim or attribution to the group has not been proven. A level of expertise would be required to judge the distinction between simple and sophisticated attacks. Further, as technology and the ease of attacks evolves, a technique that was previously sophisticated may become commonplace; the tool must exhibit the ability to adapt to this dynamic, and not naming specific technologies assists with this.

For stated intent, the question was raised as to how “frequently” is defined; this was resolved by leaving it as an analytical decision that needs to be explained in the narrative (see later for a discussion of how analysts may need to provide definitions in their narratives). A larger issue was whether frequency was the best measure for intent. Instead an alternate measure was proposed, which uses the following thresholds:

- Low = public statements (threats)
- Medium = private / internal statements (proposals)
- High = private / internal statements (plans)

The tool was modified to reflect this alternate wording.

Ideological support and doctrine have a number of potential issues. For example, the question was raised as to whether there would be a group who would not support the use of cyber attacks. Another challenge could be that there may be doctrine supporting the use, but ideology may be silent on the issue. The wording was changed to reflect these issues.

Senior leadership support could be difficult to assess in situations where there no “senior leadership” exists. In addition, it was felt that the indicator would only be relevant for groups with both hierarchical command and control structures and effective internal discipline. It would therefore not be relevant for network-based groups and for groups lacking effective discipline. Further, there could be situations where there is support without encouragement. The indicator was removed.

For degree of harm, concerns were raised related to how to operationalize levels of harm (minor, medium, and significant). In addition, it was noted that a dollar amount that is significant for one organization (such as a small community group) may be considered minor for another (such as a national government). Further, including “encouraged” on equal footing as attempted and carried is problematic because it equates aspirational intent with actual activities. The indicator was modified to require concrete actions, shifting “encouraged” to “planned”. Further it was moved to Tier One.

Without concrete examples, there was some difficulty understanding what was meant by the use of cyber as a tactical tool and why tactical was being used and not strategic. Ultimately the indicator was modified to focus on the acceptability of using cyber attacks; specifically, the situations in which cyber attacks may be used.

Complexity raised some questions, particularly whether demonstrated skills would include the skills demonstrated in attempted and successful attacks as well as conspiracies that were stopped. Also, might there be other acceptable demonstrations of skill that apply? The indicator was changed to sophistication.

Target access for inside information could include corruption of insiders as well as infiltration by group members, supporters or agents. However, this double-scores infiltration. The solution was to move infiltration to target access for insider information.

Finally, regarding external sponsorship, questions were raised regarding whether sponsorship by a sub-national group is necessarily less effective than sponsorship by a nation state. A nation-state with few resources could be a less effective sponsor than a sub-national group with extensive resources. Thus, rather than including the identity of the sponsor, the indicator should measure the sponsor's cyber threat-related resources and capabilities.

Unknowns

There was quite a bit of discussion about how to handle “unknowns”, with a number of issues and options discussed. For example, should unknown be scored high as well (the so-called “unknown-unknowns”)? It was noted that what isn't known can be just as dangerous; it may be what tips the whole scale. Therefore, the need to find out becomes very compelling. Thus, unknowns identify gaps that need to be filled. In addition, it is important that if there are not enough other indicators to determine the appropriate level, in the narrative the analyst would state that they have unknowns that need to be filled.

Focus Group

General Discussion

The following section reports on the discussions amongst, and arguments made by, the focus group participants. In concurrence with the modified Chatham House rules in place for the focus group, the information herein is presented in the aggregate exclusive of all potential identifiers of individual or organizational attributions.

Discussion in the focus group opened with a reminder from the participants themselves to be mindful that the threat being examined was that of cyber threat. The question was raised as to whether both physical and cyber threats should be looked at together, but it was noted that when examining something “weird” it is helpful to have a separate tool. While the ideal situation would be to examine all threats together, the reality is that a country or agency may not be set up to do that. In that context, the participants felt that it was better to have separate tools then aggregate the assessments afterwards. They believed that, provided the “building blocks” were present and that a proper context was established, then this represented a better approach.

Participants discussed the definition of cyber threat given on the first page of the tool. They noted that it clearly placed the focus of the tool on the threat agent and not on any particular threat event. Further, they liked that the definition of cyber threat was “bounded”.

Some discussion revolved around why the tool was so specific to cyber threats, and there was speculation on whether the tool could be used for other purposes. The participants decided that because this will be a multi-attribute decision support tool it

may be adaptable for other uses, such as assessment of the organized crime cyber threat. However, they suggested that use of a separate tool would be preferred because of the differences between the two, including the existence of items that would not be applicable to one or the other. It was also noted that the option of “not applicable confuses analysts” and so the fewer instances that exist the easier it would be use the tool.

An Expert-Based Scientific Structured Analytical Technique

Analytical challenges were referred to in the context of an increasing requirement for analysts to demonstrate how they know something – to answer the question “how do you know that?” Coupled with this is the expectation that an analyst will be able to defend their knowledge. Participants believed that the structure of the tool gives reliability and that it promotes inter-answer reliability. They noted that it is challenging to communicate a threat without a structure. As an example, participants discussed how threat agent capability is defined. While an analyst’s objective assessment may be used, inherently the perceptions of other actors are able to be subsumed into some of the indicators. This type of assessment is already conducted of criminals on a regular basis. For example, a criminal threat assessment may state that Person Z takes drugs and thinks they can rob a bank, but they lack the tools and resources required, so when they attempt to rob banks they are unsuccessful.

Participants noted that having attributes (indicators; the tool) compiled by people who know what they are doing turns it into an expert consensus; the tool is thus an expert-based scientific structured analytical technique. This, in turn, gives the agency

management confidence that an analyst has not been biased, that a reasonable objective scientific approach has been undertaken.

Analysts are not the only source of bias. Intelligence assessment consumers, such as managers, also have biases. Participants noted that using an expert-based scientific structured analytical technique limits the ability to shift an assessment to achieve a particular desired outcome, which in turn reduces pressure to steer the assessment in one direction or another. A number of elements work together to this end: defined attributes that are difficult to manipulate and that have clear parameters give the tool and analyst strength. The threat assessment is able to stand in part because there is a methodology, it is sound and transparent. In this way, a structured analytical tool, strong analysis, and strong management all work together to allow the analysis to stand and neither be steered nor changed.

The Narrative

Because the tool is not a threat assessment, and the accompanying narrative is, participants requested an indicator worksheet template (Annex A in Appendix D) be added to the tool. The purpose of this worksheet was to guide or remind analysts in the collection and documentation of facting information supporting their narrative, as well as assist with the narrative itself. They felt such a worksheet would be particularly useful for junior analysts and for situations when large volumes of information must be assessed. The worksheet will allow the analyst to clearly articulate “this is where we’re at” via documentation of the available information. It also allows collaboration, serves as a collation and assessment tool, and allows one to go back and see a shift in group

and cyber techniques over time. While there was an initial suggestion that the worksheet could be in spreadsheet format, it was eventually decided that leaving it in the word processing format would allow for greater flexibility.

In their experience, participants have found that it is incredibly difficult to put together a holistic assessment. They believe that this tool will help with that process. However, they also pointed out that a culture must be conveyed to senior management that this type of information is needed, that one has a need to know what one is protecting and from what one is being protected. Threat-based risk management is driven by threats against assets. An example was given that while it is very easy to have a door or a lock, how do you know you need them in the first place? This tool provides a systematic way of gathering the relevant information and assessing it to the appropriate conclusion.

The Instrument

The bulk of the focus group discussion was related to the instrument itself. This initial part of the discussion began moving randomly around the instrument and the various indicators before moving into a sequential examination of each indicator. Key issues raised during the first part of the discussion included:

- Whether an attack on one country is an indicator of attack likelihood against another.
- Terrorists monitor others and learn; therefore, an event happening elsewhere may indicate a trend.
- Sophistication speaks to the ability to surprise us.

- Indicators are really questions:
 - ❖ Are they willing to do this?
 - ❖ Have they done this?
 - ❖ Are they planning on doing it?

Participants liked that the indicators were ordered from unknown to high rather than from high to unknown.

Participants were particularly concerned with how to handle “unknown” as a valid response. On the final Threat Table there is no unknown option for either intent or capability. However, management needs to know if actual unknowns exist. Participants specifically stressed the importance of the narrative when dealing with unknowns, stating that clear guidance was needed in the instrument for how the analyst was to handle the situation in the overall assessment when the intent or the capability are unknown. New wording was added to this section:

Unknowns represent intelligence gaps. Analytical judgement determines when the group/individual as a whole represents an intelligence gap that cannot be assessed. This table cannot be used if either intent or capability are assessed as unknown. In such a case, the assessment itself must be used to clearly state the level that is known and that the other is unknown.

Later in the day, further discussion about intent and capability led to an examination of their relative weights and the inclusion of further language to the Threat Table section. Participants argued that while it is more difficult to establish or change capabilities than intent, intent has been shown to be stronger influence over the overall level; it is a necessary but not sufficient condition. Without intent, there will be no attack. Intent, therefore, ultimately determines if an attack occurs, all other factors remaining the same.

Participants also discussed parts of what are necessary in the accompanying narrative. For example, a confidence statement – a statement of how confident the analyst is in their findings – is needed in the narrative; in many cases it is one of the first things stated. Also, analysts need to present their information in a language the audience will understand, which may include providing definitions of terms used. The participants explained that while conducting the assessment and using the tool may be daunting the first time, once one “gets into it” one will likely realize its benefits. It will provide a better method of collation, which in turn will facilitate analysis. One participant speculated that in the future one could create a heat map of the overall data, which could be a way to present findings to management. Further, one of the advantages of the tool was the ability to understand the impact of what happens if there is a change in an indicators. If the analyst takes their time, this will allow for “what if” analysis to occur.

The Indicators

When the discussion of indicators occurred, one indicator evoked significant dialog: “Cyber Attack History”. This indicator is unique because it is about what is known to have been done; it is fact-based, whereas the other indicators relate to what terrorists want, hope, or plan to do. For this reason there was quite a bit of discussion as to whether this indicator should be removed from Intent and Capability entirely and form its own Tier 1 attribute, it being neither an intent nor a capability. Ultimately, the participants decided to leave it as a Tier 1 Intent indicator. There was then discussion about the use of frequency as part of the indicator. It was noted that if frequency is used and it always creates an intelligence gap, the indicator becomes useless.

Therefore, the discussion then shifted into how to rework the indicator level wordings. If there is an attack history, there is an applicable rating of some sort; there are also measures of harm (which is another indicator). The final decision was to use wording reflective of none, planned, attempted, and successful.

The remainder of the discussion about indicators revolved around making refinements to the wording or indicator title. Table 4.7 lists these changes and comments. “Unknown” became defined as “unable to assess”.

Table 4.7 Indicators: Changes and Comments

| Indicator | Change & Comments |
|---|---|
| Stated intent to conduct cyber attacks | Participants liked that the indicator refers to “confirmed private communication” |
| Degree of harm | Add “against CountryA targets”. Don’t have levels of harm in each category defined; this avoids the need to try to scale number of lives lost versus monetary loss. |
| Cyber attack history (non-CountryA targets) | Use the same language as Cyber attack history, except insert non-CountryA |
| Doctrine | Add “normal operating procedures” |
| Innovation | Add “methods and”.... |
| Technical resources | Rename “human resources”. “cyber attack methods” drop “methods”. |
| Target information collection | Change title to “information collection on target(s)” |
| Target access for insider information | Change title to “access to insider information on target(s)” |
| Target scope | Integrate concept of sequential, simultaneous, and multiple sequential cyber attacks. |
| Collaboration | For none, change links to collaboration. This indicator is separate from sponsorship. |

Threat Table

The final discussion related to the instrument involved the threat table.

Participants explained that based on prior experience with similar kinds of visual tables,

the muted pastel colours I had chosen, while aesthetically acceptable, did not sufficiently convey the resulting overall threat assessment. Instead, they directed that specific colours be used, as indicted in Table 4.8. During the focus group, the participants helped with appropriate shade selections from the word processor menus.

Table 4.8 Threat Table Colors

| Threat Level | Colour |
|--------------|-------------|
| VERY HIGH | RED |
| HIGH | YELLOW |
| MEDIUM | ORANGE |
| LOW | GREEN |
| VERY LOW | BRIGHT BLUE |
| NONE | NO COLOR |

Validation of the Instrument: Vignette Assessments

Focus group participants conducted two assessments of the cyber threat posed by the hypothetical vignettes of fictional organizations and individuals. The first, conducted first thing in the morning, was an individual exercise where participants were asked, using their professional experience and opinion, to conduct an assessment of each fictional vignette (Appendix C), and to indicate in the provided table their assessment of the level of cyber threat each organization or individual would represent to CountryA. The results of these scorings are contained in Table 4.9. Although the distribution of threat level assessments group together, there was a noticeable spread for each vignette: the greatest spread was for vignette two, that of PersonA, whose assessment ranged from very low to high, spanning across four levels.

Table 4.9 Individual Vignette Assessment Results

| | Number of participants selecting threat level | | | | |
|--|---|--------------------------|----------------------------|---------------------------------|---------------------------|
| | VIGNETTE | | | | |
| THREAT LEVEL | ONE (OrganizationA) | TWO (PersonA) | THREE (PersonB) | FOUR (OrganizationC) | FIVE (PersonC) |
| VERY HIGH | | | | 1 | |
| HIGH | 1 | 1 | | 5 | 2.5* |
| MEDIUM | 3 | 3 | | | 2.5* |
| LOW | 2 | 1 | 3 | | |
| VERY LOW | | 1 | 1 | | |
| NONE | | | 2 | | |
| UNKNOWN | | | | | |
| *One participant placed their marker on the line between high and medium; therefore, 0.5 was allocated to each level | | | | | |

At the end of the focus group day, once the analytical tool instrument had been finalized, the participants revisited the vignettes. This time, the assessment was conducted as a unified group using the newly finalized tool. The results of this assessment are represented in a modified version of the Assessment Tables in Table 4.10. As a result of their assessment, the participants noted that there was an intelligence gap existent with respect to the capabilities of OrganizationA.

In contrast to the individual assessments, the unified group was in agreement as to the indicators' levels and the overall threat level. Their overall assessment also differed from the individual assessments, with some vignettes being assessed higher, others lower. This difference in overall assessment, in the real world, could have a significant impact on decision-makers, the allocation of resources, and the direction investigations take. Participants said they felt more confident with the results of the assessment using the instrument as finalized. In addition, participants commented that while extraneous information can have a great influence when doing an assessment "by gut", using a structured tool allows for the realization that some information is actually

not relevant. One participant commented on how very different his/her assessments were between the individual assessment and the group assessment. The participant noted that there were a number of issues the tool raised in the form of indicators that the participant had not thought to consider when they were conducting the assessment alone and without benefit of the tool.

In their closing comments, participants anticipated that as the instrument gets used “live” in the future, it will get updated with the lessons that can only be learned from applying it to real data, in real situations. They also explained that a tool like this would be almost impossible to create within the aegis of an intelligence bureaucracy, though it may be able to be created “off the side of your desk”.

Final Questionnaire

The last task the participants completed as part of the focus group was a survey which asked to what extent they agreed with a series of questions related to their experience assessing the fictional vignettes (both with and without the analytical tool), and their experience using structured analytical techniques/tools, based on their professional experience and opinion. The survey questions used a five-point scale (strongly agree, agree, neither agree nor disagree, disagree, strongly disagree) for each question. Five participants completed the final survey.

Table 4.10 Results of Group Assessment of Vignettes

| | | Vignette Assessed*** | | | | |
|--|---|----------------------|---------|----------|-----------|-----------|
| | | Org. A | Pers. A | Pers. B | Org. C | Pers. C |
| OVERALL THREAT LEVEL | | LOW | MEDIUM | VERY LOW | VERY HIGH | VERY HIGH |
| Indicators | OVERALL INTENT | LOW | HIGH | LOW | HIGH | HIGH |
| | INTENT – TIER ONE | | | | | |
| | CYBER ATTACK HISTORY | None | High | None | High | Unknown |
| | STATED INTENT TO CONDUCT CYBER ATTACKS | Low | High | Low | High | High |
| | DEGREE OF HARM | None | Medium | None | Medium | Medium |
| | INTENT – TIER TWO | | | | | |
| | CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | None | Unknown | None | None | Unknown |
| | IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | Low | High | Low | High | High |
| | ACCEPTABLE USE OF CYBER ATTACKS | Unknown | High | Unknown | Unknown | Unknown |
| | OVERALL CAPABILITY | LOW | LOW | NONE | HIGH | HIGH |
| | CAPABILITY – TIER ONE | | | | | |
| | TECHNICAL EXPERTISE | Low | Low | None | High | Medium |
| | SOPHISTICATION | None | Low | None | High | Unknown |
| | INNOVATION | Unknown | None | None | Unknown | Unknown |
| | CAPABILITY – TIER TWO | | | | | |
| | HUMAN RESOURCES | None | Low | None | High | High |
| | INFORMATION COLLECTION ON TARGET(S) | Unknown | Unknown | None | Unknown | Unknown |
| | ACCESS TO INSIDER INFORMATION ON TARGET(S) | Unknown | None | None | Unknown | Unknown |
| | TARGET SCOPE | None | None | None | Medium | Unknown |
| | COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | None | None | None | Medium | High |
| | EXTERNAL SPONSORSHIP | None | None | None | Unknown | None |
| **Org. A” = OrganizationA; “Pers. B” = PersonB, etc. | | | | | | |
| **The indicator rankings determining the overall rankings are shaded gray. | | | | | | |

The results of the survey were quite uniform. Overall, participants found the tool to be of value. They also believed that structured analytical tools are of value. In particular, participants:

- Strongly disagreed (two) or disagreed (three) that the vignettes were easier to assess when NOT using the analytical tool.
- Strongly agreed (four) or agreed (1) that the vignettes were easier to assess when USING the analytical tool.
- Disagreed (four) or strongly disagreed (one) that assessing the vignettes with and without the analytical tool were of equal difficulty.
- Believed that the analytical tool would help guide the cyber threat assessment of terrorist organizations and individuals (three strongly agree, two agree).
- Believed the analytical tool would bring positive value to the cyber threat assessment of terrorist organizations and individuals (five strongly agree).
- Believed that structured analytical techniques/tools help guide the assessment of terrorist organizations and individuals (three strongly agree, one agree, one no response).
- Believed that structured analytical techniques/tools bring positive value to the assessment of terrorist organizations and individuals (three strongly agree, one agree, one no response).

All four of the participants who responded to this particular question have, in the past, used structured analytical techniques/tools to assist in the assessment of criminal organizations or individuals, or terrorist organizations or individuals. Finally, of the four who responded to the question, when they conduct assessments of criminal

organizations or individuals, or terrorist organizations or individuals, participants answered that they make use of a structured analytical technique every time (one), almost every time (two), or occasionally/sometimes (one).

CHAPTER FIVE

CONCLUSION

This study successfully leveraged the experience of professional experts to develop a new functional construct: a qualitative analytical technique designed to assess the cyber threat posed by terrorist entities and individuals. The final instrument (Appendix D) is a novel structured analytical construct that uses defined indicators of a terrorist entity/individual's intent to carry out cyber attacks, and their capability to actually do so as measures of an entity/individual's overall level of cyber threat.

Participants were able to answer three fundamental research questions: what the structure of the instrument should look like, what it should contain, and what other material should accompany it. More importantly, they also validated the concept of the tool and its usefulness in support of professional analysis as an expert-based scientific structured analytical technique.

Structure

Although additions were made to the instrument, the fundamental structure remained the same. At a simple level, because threat is a function of intent and capability, the construct had to contain both elements. However, participants supported the two innovations which were made when the prototype was created:

- Separate intent and capability, have indicators for each, and determine an overall level for each, which are then brought together to inform the overall level of threat.
- Create a tier structure which puts more weight on some indicators over others.

While conducting a search of the literature for relevant works, I came across many assessment instruments intended for various purposes. Many consisted of just a matrix with check-boxes to select, with little to no explanation on how use of the matrix let alone operational definitions for terms used as well as what information needed to accompany it. These types of instruments are problematic not only because they run the risk of being used improperly or in inappropriate situations, but also because they suffer from reliability issues, particularly when attempting to compare assessments between analysts.

This study's final construct is a functional instrument with extensive documentation to guide analysts on how the tool is used. In addition, it stresses how important an accompanying narrative is. As noted by the participants, the assessment is not the tool, the assessment is the narrative. The tool's role is to support that assessment and facilitate the creation of the narrative.

Indicators

The separation of indicators into intent and capability groupings created some challenges, primarily related to ensuring that the title, definition, and ratings of each indicator were confined to just intent or just capability. Participants highlighted the importance of not accidentally double-counting information, because it imparts uneven weight from indicators, thus rendering many of the assessments unreliable..

Input into what the indicators should be took the bulk of the participants' time as the indicators have the most significant impact on the overall outcome when the instrument is used. Although some of the wording changes may only be a word or two,

the nuances of the change often had a significant impact on the meaning or on how the indicator would be assessed. Larger changes made the tool more effective by removing redundancy, narrowing and clarifying definitions, and providing rating options which were discrete and able to be assessed.

Additional Material

A vital contribution of the participants was their direction for the inclusion of additional material. An example Assessment Table provides guidance to analysts on how indicator ratings interact to contribute to overall intent and capability levels, which in turn inform the overall threat level. Participants felt this was necessary for the reduction of confusion on the part of analysts who may better understand how the interrelationships exist when presented with a visual demonstration. The indicator worksheets provide clear guidance and reminders to analysts to ensure their analysis is supported with relevant information and evidence, that this support is well-documented, and that a narrative is created.

Validation

The expert consensus of the participants was that the final instrument was a valuable contribution to the field, that it would be a useful tool for analysts, and that it would support and strengthen analytical assessments by providing an expert-based structured analytical methodology for analysts to employ. In turn, analysts would be producing assessments that were more robust, reliable, and less prone and susceptible

to external influence than existing practices which do not make use of structured methods.

While fictional vignettes were used to validate the tool in this study, it is anticipated that the use of information about real terrorist entities and individuals would result in a similar validation. Repeated use with real world data, however, is likely to identify additional ways in which the instrument can be improved. Rather than a static instrument, it is understood that the instrument will continue to evolve as it is put into use and as a wider audience of professionals is able to examine it. Additionally, the dynamic nature of the instrument will allow for incorporation of new indicators and/or nuances of indicators that emerge with future developments in both the technological aspects of cyber terrorism as well as the ever-evolving methodologies employed in intelligence gathering.

One of the limitations of this study is that the number of participants was small. While the size facilitated and encouraged collaborative discussion, it did limit the diversity of opinions which may have influenced the outcome of the final instrument.

The Future

The final instrument may be considered the “beta” version of the construct. The next logical step is for the tool to be tested against data regarding real terrorists. It may be possible to conduct this validation from with a well-constructed academic study; otherwise, the results would remain within government circles. If validated, it would then be appropriate for the tool (or a modified version of it, if/when the need for

modifications was identified) to be introduced to a wider group of experts to try with real data and to review for consideration of revision.

Despite the artificialities of the study context, the success of this process suggests that a similar process (or one modified for a working environment as opposed to an academic setting) could be used to engineer similar instruments to examine other threat areas about which there is uncertainty.

APPENDIX A

PROTOTYPE ANALYTICAL TOOL INSTRUMENT

INTRODUCTION

This structured analytical tool is used to assist analysts in assessing the level of cyber threat posed by terrorist organizations and individuals to CountryA.¹ It provides a structured way of assessing the threat, and in addition to an overall threat level, the tool can be used to assist in the development of an assessment narrative to accompany the tool's result.

Threat is composed of two components: intent and capability. That is, the terrorist organization/individual's intent to carry out cyber attacks, and their capability to actually do so.

To assess intent and capability, a number of indicators of each have been identified. Each indicator is defined. Each indicator then has defined levels of "high", "medium", "low", "none", and "unknown". Within both categories of intent and capability, the indicators are divided into "tier 1" and "tier 2" indicators. The two tiers are used to help develop an overall level to assign to intent and to capability. The overall levels of intent and capability are then compiled together to form the overall threat level of the assessment.

HOW TO USE THE TOOL

Each terrorist organization or individual is assessed individually. Once assessed, groups and individuals may be compared to each other, or compared to themselves over a period of time.

The tool is worded to assess a general cyber threat. However, it is possible to specify a specific type of cyber threat, a specific target, a specific time horizon, or a different country or more specific location, by adding the appropriate words to the appropriate indicators. When reporting on an assessment using this tool, an indication of this type of specificity should be included.

A supporting narrative should accompany any assessment using this tool. The narrative would typically include explanations, justifications, considerations, and an indication of certainty for how the indicators were assessed. The narrative may also include a discussion of the impact that changes to specific indicators may have on the overall assessment.

¹ "CountryA" is used as a placeholder for the reference country. In actual use, the country of concern (e.g. Canada, United states, United Kingdom) would be used in place of "CountryA".

To use the tool:

1. Choose the terrorist organization or individual to assess;
2. Assess a level (high, medium, low, none, unknown) for each indicator, as it applies to the terrorist organization/individual being assessed;
3. Determine the overall level for each of INTENT and CAPABILITY, using the following rules:
 - a. The overall level is the highest level indicated by either of:
 - i. ONE tier 1 indicator; or
 - ii. TWO tier 2 indicators
4. Using the overall levels for INTENT and CAPABILITY, select the appropriate overall threat level from the Threat Level Table.
5. A supporting narrative should accompany any assessment using this tool.

INDICATORS

Each indicator is arranged using the following outline, consisting of an indicator name, its definition, and defined levels:

| INDICATOR NAME | Definition of indicator. | |
|----------------|--------------------------|--|
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Definition of none for indicator. |
| | LOW | Definition of low for indicator. |
| | MEDIUM | Definition of medium for indicator. |
| | HIGH | Definition of high for indicator. |

INTENT INDICATORS – TIER ONE

| | | |
|---|---|---|
| CYBER ATTACK HISTORY | The extent to which cyber attacks have previously been committed against CountryA targets, including conspiracies, attempts, and successful attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No demonstrated use of cyber attacks against CountryA targets. |
| | LOW | Demonstrated use of simple cyber attacks methods against CountryA targets (such as website defacements, denial of service attacks). |
| | MEDIUM | Demonstrated use of sophisticated cyber attacks against CountryA targets without intent to cause significant physical, monetary or information losses. |
| | HIGH | Demonstrated use of sophisticated cyber attacks against CountryA targets with intent to cause or actual significant physical, monetary or information losses. |
| STATED INTENT TO CONDUCT CYBER ATTACKS | The stated intent (publically or through confirmed private communications) to conduct cyber attacks against CountryA targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No stated intent to commit cyber attacks against CountryA targets. |
| | LOW | Occasionally stated intent to conduct cyber attacks against CountryA targets. |
| | MEDIUM | Frequently stated intent to conduct simple cyber attacks against CountryA targets. |
| | HIGH | Frequently stated intent to conduct sophisticated cyber attacks against CountryA targets. |

INTENT INDICATORS – TIER TWO

| | | |
|--|---|--|
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | The extent to which the use of cyber attacks are encouraged or permitted by motivating ideology and supporting doctrine. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No support for cyber attacks in ideology and doctrine. |
| | LOW | Ideology supports use of cyber attacks, but there is no supporting doctrine for their use. |
| | MEDIUM | Both ideology and doctrine support some use of cyber attacks. |
| | HIGH | Both ideology and doctrine strongly support and encourage use of cyber attacks. |
| SENIOR LEADERSHIP SUPPORT FOR CYBER ATTACKS | The extent to which the senior leadership of the organization supports and encourages the use of cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Senior leadership does not support and actively discourages the use of cyber attack. |
| | LOW | Senior leadership is undecided or neutral about the use of cyber attacks. |
| | MEDIUM | Senior leadership support and encourages the use of cyber attacks. |
| | HIGH | Senior leadership strongly supports and encourages the use of cyber attacks. |
| DEGREE OF HARM | The degree of cyber attack harm encouraged, attempted, or carried out. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No harm. |
| | LOW | Minor monetary or information losses. |
| | MEDIUM | Moderate physical, monetary or information losses. |
| | HIGH | Significant physical, monetary or information losses. |

| | | |
|--|---|---|
| TACTICAL USE OF CYBER ATTACKS | How cyber attacks are to be used as a tactical tool. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Cyber attacks are unacceptable. |
| | LOW | Cyber attacks are only to be used as a defensive tool. |
| | MEDIUM | Cyber attacks are an offensive tool only under limited circumstances. |
| | HIGH | Cyber attacks are an offensive tool under all circumstances. |

CAPABILITY INDICATORS – TIER ONE

| | | |
|----------------------------|---|--|
| TECHNICAL EXPERTISE | The extent of demonstrated technical expertise for conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No technical expertise. |
| | LOW | Some theoretical technical expertise but no or limited practical use of cyber attack methods. |
| | MEDIUM | Extensive theoretical expertise but no or limited practical use of cyber attack methods OR extensive practical use but limited theoretical knowledge. |
| | HIGH | Extensive theoretical knowledge AND extensive practical experience, at a level comparable to professional expertise in cyber attack methods. |
| COMPLEXITY | The extent to which a complex cyber attack can be carried out. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No capability and no previous attacks. |
| | LOW | Demonstrated skills to plan and carry out simple attacks. |
| | MEDIUM | Demonstrated skills to plan and carry out complex attacks, but no prior successful complex attacks. |
| | HIGH | Demonstrated skills to plan and carry out complex attacks, and history or prior successful complex attacks. |
| INNOVATION | Ability to innovate and independently develop new cyber attack tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to use or develop new cyber attack tools. |
| | LOW | Ability to use but not independently develop cyber attack tools; reliant on tools developed by others. |
| | MEDIUM | Ability to independently develop some cyber attack tools, but dependent on others for most cyber attack tools. |
| | HIGH | Ability to independently develop most or all cyber attack tools required. |

CAPABILITY INDICATORS – TIER TWO

| | | |
|----------------------------|--|---|
| TECHNICAL RESOURCES | Extent of human resources that are dedicated to cyber attack methods. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No resources dedicated to cyber attack methods. |
| | LOW | Only individuals working independently are dedicated to cyber attack methods. |
| | MEDIUM | A single unit of a few individuals is dedicated to cyber attack methods. |
| | HIGH | A large single unit or multiple units are dedicated to cyber attack methods. |

| | | |
|--------------------------------------|---|--|
| TARGET INFORMATION COLLECTION | Methods for information gathering about prospective targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Conduct no information gathering about prospective targets. |
| | LOW | Basic information gathering, largely limited to public open source information. |
| | MEDIUM | Moderate information gathering, including use of social engineering methods. |
| | HIGH | Sophisticated information gathering, including multiple methods such as directed social engineering, insider information, and/or advanced persistent threat methods. |

| | | |
|---------------------|--|--|
| TARGET SCOPE | Ability to conduct sophisticated cyber attacks against multiple simultaneous targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to conduct attacks against multiple targets. |
| | LOW | Ability to conduct simple attacks against multiple targets. |
| | MEDIUM | Ability to conduct sophisticated cyber attacks against a limited number of multiple targets. |
| | HIGH | Ability to conduct sophisticated cyber attacks against as many targets as desired. |

| | | |
|--|---|--|
| LINKS TO OTHER CRIMINAL EXTREMISTS CONDUCTING CYBER ATTACKS | Extent of links to other criminal extremists conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No links. |
| | LOW | Some links, but no known exchange of information regarding cyber attack training, tools, and best practices. |
| | MEDIUM | Some links, including limited exchange of information regarding cyber attack training, tools, and best practices.. |
| | HIGH | Strong links, including extensive exchange of information regarding cyber attack training, tools, and/or best practices. |

| | | |
|--|---|--|
| LINKS TO CRIMINALS CONDUCTING CYBER ATTACKS | Extent of links to criminals (but not other criminal extremists) conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No links. |
| | LOW | Some links, but no known exchange of information regarding cyber attack training, tools, and best practices. |
| | MEDIUM | Some links, including limited exchange of information regarding cyber attack training, tools, and best practices.. |
| | HIGH | Strong links, including extensive exchange of information regarding cyber attack training, tools, and/or best practices. |

| | | |
|--|--|--|
| TARGET ACCESS FOR INSIDER INFORMATION | Extent of infiltration of target to gain insider-level information. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | None. |
| | LOW | No demonstrated history of infiltration of targets in any capacity, but some prior attempts or plans to do so. |
| | MEDIUM | Demonstrated history of infiltration of targets in a non-technical capacity. |
| | HIGH | Demonstrated history of infiltration of targets in a technical capacity. |

| | | |
|---------------------------------|--|---|
| EXTERNAL SPONSORSHIP | Sources of resource sponsorships, including finances and cyber attack training and tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No external sponsorship. |
| | LOW | Sponsored by sub-national groups or individuals with limited means available. |
| | MEDIUM | Sponsored by sub-national groups or individuals with extensive means available. |
| | HIGH | Sponsored by a nation state. |

ASSESSMENT TABLE – OVERALL SUMMARY

| (Name of terrorist organization/individual being assessed) | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL INTENT | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER ONE | | | | | |
| CYBER ATTACK HISTORY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| STATED INTENT TO CONDUCT CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER TWO | | | | | |
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SENIOR LEADERSHIP SUPPORT FOR CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| DEGREE OF HARM | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TACTICAL USE OF CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| | | | | | |
|---|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| OVERALL CAPABILITY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 1 | | | | | |
| TECHNICAL EXPERTISE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| COMPLEXITY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INNOVATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 2 | | | | | |
| TECHNICAL RESOURCES | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET INFORMATION COLLECTION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET SCOPE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| LINKS TO OTHER CRIMINAL EXTREMISTS CONDUCTING CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| LINKS TO CRIMINALS CONDUCTING CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET ACCESS FOR INSIDER INFORMATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| EXTERNAL SPONSORSHIP | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

THREAT LEVEL TABLE

Using the following table, plot the overall level for each of INTENT and CAPABILITY to determine the overall assessment threat level:

| | | CAPABILITY | | | |
|--------|--------|------------|----------|----------|-----------|
| | | NONE | LOW | MEDIUM | HIGH |
| INTENT | NONE | NONE | VERY LOW | VERY LOW | LOW |
| | LOW | VERY LOW | LOW | LOW | MEDIUM |
| | MEDIUM | LOW | MEDIUM | MEDIUM | HIGH |
| | HIGH | LOW | MEDIUM | HIGH | VERY HIGH |

APPENDIX B

REVISED ANALYTICAL TOOL INSTRUMENT

INTRODUCTION

This structured analytical tool is used to assist analysts in assessing the level of cyber threat posed by terrorist organizations and individuals¹ to CountryA.² It provides a structured way of assessing the threat, and in addition to an overall threat level, the tool is used to assist in the development of an assessment narrative to accompany the tool's result.

Threat is composed of two components: intent and capability. That is, the terrorist organization/individual's intent to carry out cyber attacks, and their capability to actually do so. For the purpose of this tool, "cyber attacks" are the use of cyber methods as a means to attack cyber targets (although a physical target (such as a physical system controlled by a computerized device) may be the ultimate intended target, "cyber attacks" are conducted through cyber rather than kinetic means against physical targets). The tool is NOT intended to examine computer-enabled crime nor other supportive use of information technologies where computers are not the method, means, and target of attack.

To assess intent and capability, a number of indicators of each have been identified. Each indicator is defined. Each indicator then has defined levels of "high", "medium", "low", "none", and "unknown". Within both categories of intent and capability, the indicators are divided into "tier 1" and "tier 2" indicators. The two tiers are used to help develop an overall level to assign to intent and to capability and reflect indicators that very strongly contribute to the category level, and indicators that less strongly contribute. The overall levels of intent and capability are then compiled together to form the overall threat level of the assessment.

HOW TO USE THE TOOL: GENERAL INFORMATION

The tool is not intended to be used as a stand-alone assessment. In addition to providing a picture of the overall cyber threat level, the tool is an aid to judgement – it is used to assist in the development of an accompanying assessment narrative. This overall assessment is based on the information available at the time it is conducted, with the narrative is used to qualify, provide context, and state the analytical judgements. A more detailed discussion of the narrative follows in the next section.

Each terrorist organization or individual is assessed individually. Once assessed, groups and individuals may be compared to each other, or compared to themselves over a period of time.

¹ "terrorist organizations and individuals" refer to organizations and individuals who meet the definition of "terrorist group" under the Criminal Code of Canada, Section 83.01 (or corresponding law in the country making use of the tool) and similarly motivated organizations/individuals who act within the cyber realm.

² "CountryA" is used as a placeholder for the reference country. In actual use, the country of concern (e.g. Canada, United States, United Kingdom) would be used in place of "CountryA".

The tool is worded to assess a general cyber threat. However, it is possible to specify a specific type of cyber threat, a specific target (e.g. by company, location, type of asset, specific device as a target, etc), a specific time horizon, or a different country or more specific location, by adding the appropriate words to the appropriate indicators. When reporting on an assessment using this tool, an indication of this type of specificity should be included.

HOW TO USE THE TOOL: NARRATIVE

The accompanying narrative is an essential element when using the tool. The narrative states the analytical judgements. It provides context to understand those judgements. It describes and qualifies the information used to conduct the assessment, explains its source(s), and speaks to its reliability and validity. The narrative includes illustrative examples and explanations or justifications for why indicators were judged at the level they were, including the thresholds used for specific indicators. It gives the rationale for assumptions that were made, and it highlights alternative judgements if those assumptions are incorrect. It explains situations where contradictory information gives rise to the insufficient information for assessment and thus an “unknown”. It identifies intelligence gaps, and identifies opportunities to fill those gaps and strengthen knowledge in other areas.

The supporting narrative must discuss the “unknowns” and the intelligence gaps they represent. If there are sufficient unknowns, this aspect of the organization/individual becomes an intelligence requirement.

Narrative Examples (fictional)

Cyber attack history: HIGH. In January 2014, GroupX conducted two sophisticated cyber attacks against multiple well-protected government and private sector targets in Country A. Although the attacks were intended to cause disruption of critical infrastructure such as power outages and widespread government computer system failures, the results of the actual attacks were more limited in scope, causing... The sophisticated methods and tools used included...

Degree of Harm: HIGH. In December 2013 and again in February and March 2014, the senior leadership of GroupZ again encouraged their cyber corps to focus on attacks which results in loss of life instead of attacks to support fundraising that some members of the corps had been advocating. One attack was attempted in April 2014, targeting the traffic light control system of CityX. While the intent of the attack was to cause numerous fatal traffic accidents, the attack was unsuccessful.

External Sponsorship: LOW. In 2013, GroupV received US\$3,000 from CountryY to support its cyber corps. GroupV used the funds to purchase a new laptop computer from XYZCorp.

This tool can be used by an analyst alone or a group of subject matter experts.

To use the tool:

1. Identify the terrorist organization or individual to assess;
2. Assess a level (high, medium, low, none, unknown) for each indicator, as it applies to the terrorist organization/individual;
3. Determine the overall level for each of INTENT and CAPABILITY, using the following rules:
 - a. The overall level is the highest level indicated by either of:
 - i. ONE tier 1 indicator; or
 - ii. TWO tier 2 indicators
 - b. Analytical judgement must be used to determine appropriate thresholds for some indicators (the threshold used should be explained in the narrative).
4. Using the overall levels for INTENT and CAPABILITY, select the appropriate overall threat level from the Threat Level Table.
5. A supporting narrative should accompany any assessment using this tool.

INDICATORS

Each indicator is arranged using the following outline, consisting of an indicator name, its definition, and defined levels:

| | | |
|-----------------------|--------------------------|--|
| INDICATOR NAME | Definition of indicator. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Definition of none for indicator. |
| | LOW | Definition of low for indicator. |
| | MEDIUM | Definition of medium for indicator. |
| | HIGH | Definition of high for indicator. |

INTENT INDICATORS – TIER ONE

| | | |
|---|---|--|
| CYBER ATTACK HISTORY | The extent to which cyber attacks have previously been committed against CountryA targets, including successful attacks, attempted attacks, foiled conspiracies, and non-criminal demonstrations of skill (such as formal cyber wargames). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No demonstrated use of cyber attacks against CountryA targets. |
| | LOW | Demonstrated use of crude cyber attacks methods against CountryA targets (such as website defacements, denial of service attacks). |
| | MEDIUM | Demonstrated use of sophisticated cyber attacks against poorly or moderately protected CountryA targets. |
| | HIGH | Demonstrated use of sophisticated cyber attacks against well-protected CountryA targets. |
| STATED INTENT TO CONDUCT CYBER ATTACKS | The stated intent (publically or through confirmed private communications) to conduct cyber attacks against CountryA targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No stated intent to commit cyber attacks against CountryA targets. |
| | LOW | Has made public statements or threats to conduct cyber attacks against CountryA targets. |
| | MEDIUM | Has made internal statements proposing or discussing the desirability of cyber attacks against CountryA targets. |
| | HIGH | Has had internal discussions and conducting planning regarding conducting cyber attacks against CountryA targets. |

| | | |
|-----------------------|--|--|
| DEGREE OF HARM | The degree of cyber attack harm planned, attempted, or carried out. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No harm. |
| | LOW | Embarrassment or minor monetary or information losses. |
| | MEDIUM | Physical damage including significant disruption to critical infrastructure (e.g. causing power outages) or significant monetary and information losses. |
| | HIGH | Loss of human life. |

INTENT INDICATORS – TIER TWO

| | | |
|--|---|--|
| CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | The extent to which cyber attacks have previously been committed against non-CountryA targets, including successful attacks, attempted attacks, foiled conspiracies, and non-criminal demonstrations of skill (such as formal cyber wargames). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No demonstrated use of cyber attacks against non-CountryA targets. |
| | LOW | Demonstrated use of crude cyber attacks methods against non-CountryA targets (such as website defacements, denial of service attacks). |
| | MEDIUM | Demonstrated use of sophisticated cyber attacks against poorly or moderately protected non-CountryA targets. |
| | HIGH | Demonstrated use of sophisticated cyber attacks against well-protected non-CountryA targets. |

| | | |
|--|---|--|
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | The extent to which the use of cyber attacks are encouraged or permitted by motivating ideology and supporting doctrine. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No support for cyber attacks in ideology and doctrine. |
| | LOW | Ideology supports use of cyber attacks, but there is no supporting doctrine for their use. |
| | MEDIUM | Doctrine supports some use of cyber attacks. |
| | HIGH | Doctrine strongly support and encourage use of cyber attacks. |

| | | |
|--|---|---|
| ACCEPTABLE USE OF CYBER ATTACKS | Situations in which cyber attacks may be used. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Cyber attacks are unacceptable. |
| | LOW | Cyber attacks are only to be used as a retaliatory tool. |
| | MEDIUM | Cyber attacks are an offensive tool only under limited circumstances. |
| | HIGH | Cyber attacks are an offensive tool under any circumstance. |

CAPABILITY INDICATORS – TIER ONE

| | | |
|----------------------------|---|--|
| TECHNICAL EXPERTISE | The extent of demonstrated technical expertise for conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No technical expertise. |
| | LOW | Some theoretical technical expertise but no or limited practical use of cyber attack methods. |
| | MEDIUM | Extensive theoretical expertise but no or limited practical use of cyber attack methods OR extensive practical use but limited theoretical knowledge. |
| | HIGH | Extensive theoretical knowledge AND extensive practical experience. |
| SOPHISTICATION | The extent to which a sophisticated cyber attack can be carried out (includes resources needed). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No capability and no previous attacks. |
| | LOW | Demonstrated skills and resources to plan and carry out crude attacks. |
| | MEDIUM | Demonstrated skills and resources to plan and carry out sophisticated attacks, but no prior successful sophisticated attacks. |
| | HIGH | Demonstrated skills and resources to plan and carry out sophisticated attacks, and history of prior successful sophisticated attacks. |
| INNOVATION | Ability to innovate and independently develop new cyber attack tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to use or develop new cyber attack tools. |
| | LOW | Ability to use but not independently develop cyber attack tools; reliant on tools developed by others. |
| | MEDIUM | Ability to independently develop some cyber attack tools, but dependent on others for most cyber attack tools. |
| | HIGH | Ability to independently develop most or all cyber attack tools required. |

CAPABILITY INDICATORS – TIER TWO

| | | |
|--|--|---|
| TECHNICAL RESOURCES | Extent of human resources that are dedicated to cyber attack methods. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No resources dedicated to cyber attack methods. |
| | LOW | Only individual(s) working independently are dedicated to cyber attack methods. |
| | MEDIUM | A single team of a few individuals is dedicated to cyber attack methods. |
| | HIGH | A large single team or multiple teams are dedicated to cyber attack methods. |
| TARGET INFORMATION COLLECTION | Methods for information gathering about prospective targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Conduct no information gathering about prospective targets. |
| | LOW | Basic information gathering, largely limited to public open source information. |
| | MEDIUM | Moderate information gathering, including use of social engineering methods. |
| | HIGH | Sophisticated information gathering, including multiple methods such as directed social engineering, and/or advanced persistent threat or other long term penetration and collection methods. |
| TARGET ACCESS FOR INSIDER INFORMATION | Extent of infiltration of target (directly or through corruption or recruiting of employees) to gain insider-level information. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | None. |
| | LOW | No demonstrated history of infiltration of targets in any capacity, but some prior attempts or plans to do so. |
| | MEDIUM | Demonstrated history of infiltration of targets in a non-technical capacity. |
| | HIGH | Demonstrated history of infiltration of targets in a technical capacity. |

| | | |
|---------------------|--|--|
| TARGET SCOPE | Ability to conduct sophisticated cyber attacks against multiple simultaneous targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to conduct attacks against multiple targets. |
| | LOW | Ability to conduct attacks against a limited number of targets. |
| | MEDIUM | Ability to conduct cyber attacks against a limited number different types of multiple targets. |
| | HIGH | Ability to conduct cyber attacks against as many targets of different types as desired. |

| | | |
|---|--|--|
| COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | Extent of collaboration with others conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No links. |
| | LOW | Some collaboration with others, but no known exchange of information regarding cyber attack training, tools, and best practices. |
| | MEDIUM | Some collaboration, including limited exchange of information regarding cyber attack training, tools, and best practices. |
| | HIGH | Strong collaboration, including extensive exchange of information regarding cyber attack training, tools, and/or best practices. |

| | | |
|-----------------------------|--|--|
| EXTERNAL SPONSORSHIP | Sources of resource sponsorships, including finances and/or cyber attack training and/or tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No external sponsorship. |
| | LOW | Sponsor provides limited resources. |
| | MEDIUM | Sponsor provides moderate resources. |
| | HIGH | Sponsor provides extensive resources. |

ASSESSMENT TABLE – OVERALL SUMMARY

| (Name of terrorist organization/individual being assessed) | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL INTENT | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER ONE | | | | | |
| CYBER ATTACK HISTORY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| STATED INTENT TO CONDUCT CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| DEGREE OF HARM | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER TWO | | | | | |
| CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ACCEPTABLE USE OF CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| (Name of terrorist organization/individual being assessed) | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL CAPABILITY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 1 | | | | | |
| TECHNICAL EXPERTISE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SOPHISTICATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INNOVATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 2 | | | | | |
| TECHNICAL RESOURCES | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET INFORMATION COLLECTION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET ACCESS FOR INSIDER INFORMATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET SCOPE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| EXTERNAL SPONSORSHIP | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

THREAT LEVEL TABLE

Using the following table, plot the overall level for each of INTENT and CAPABILITY to determine the overall assessment threat level:

| | | CAPABILITY | | | |
|--------|--------|------------|----------|----------|-----------|
| | | NONE | LOW | MEDIUM | HIGH |
| INTENT | NONE | NONE | VERY LOW | VERY LOW | LOW |
| | LOW | VERY LOW | LOW | LOW | MEDIUM |
| | MEDIUM | LOW | MEDIUM | MEDIUM | HIGH |
| | HIGH | LOW | MEDIUM | HIGH | VERY HIGH |

Unknowns represent intelligence gaps. Analytical judgement determines when the group/individual as a whole represents an intelligence gap that cannot be assessed.

APPENDIX C
FICTIONAL VIGNETTES

The following are descriptions of five FICTIONAL terrorist organizations and individuals. Although they may resemble real organizations, they are FICTIONAL. These descriptions are used in conjunction with other study materials.

You represent CountryA. CountryA is a western country with several very close allies.

ORGANIZATION-A

Organization-A is a worldwide terrorist organization who first came into existence over 15 years ago. Inspired by an extremist religious ideology, the organization ultimately wishes to have the entire world, including all world governments, follow their religious ideology in the form of a single theocratic government. Over the past fifteen years, Organization-A has launched numerous physical terrorist attacks against governments and countries that they oppose. These attacks have included bombings, assassinations, and firearms attacks. They target government buildings and “soft” civilian targets, such as transportation services. They have, for example, successfully attacked passenger rail trains, urban buses, and commercial passenger aircraft. Organization-A has a number of experienced expert bomb-makers who are known for both the sophistication of their devices and their tendency to innovate in order to “stay ahead” of security measures. Although they plan and launch major several attacks a year worldwide, not all of Organization-A’s planned attacks have been successful. The most common reason for attack failure is the capture of the individuals involved in the attack during planning stages. Three bombing attacks in the last two years have been stopped as the attack was being carried out due to either mechanical failure of a bomb to detonate, or an error on the part of the bomber to correctly trigger the device. All of Organization-A’s successful attacks have results in at least 10 fatalities and usually over 100 injured. The two commercial passenger aircraft they blew up resulted in the deaths of all on board, 239 and 188 respectively. The frequency of their attacks has increased each year since their inception. Organization-A is a hierarchical organization whose senior leaders select and approve each attack. The group uses a cell structure to increase operational security and compartmentalize responsibilities. Although other individuals have carried out attacks who have been inspired by Organization-A’s ideology (in large part because their propaganda and some training materials are widely available on the Internet), those attacks have not been officially claimed by Organization-A. The senior leadership of Organization-A have named CountryA and its closest allies as legitimate targets for the group. CountryA is the only country among these allies to have not been directly attacked. The doctrine of and training provided by the group emphasizes the use of physical attacks. However, the group’s senior leadership has stated that they would like to be able to engage in cyber attacks in the future. Organization-A has a membership which includes many members who have university degrees, including in engineering, medicine, and the sciences. Some of these members have graduate degrees, including PhDs. Although Organization-A has approximately 12 members with community college or university-level degrees in computer science, all are believed to be currently used for logistics or bomb construction purposes.

PERSON-A

Person-A is inspired by the ideology of Organization-A. Although not a member of Organization-A, 26 year old Person-A intends to carry out an attack against CountryA that he believes will help achieve the overall goals of Organization-A. Person-A grew up in CountryA and attended a public university there, graduating with an undergraduate degree in Computer Science four years ago. Person-A resides in CountryA and has strong family and friend ties there. He works fulltime in the service industry and has had difficulty finding a job in his field as a number of high-tech companies in his area have been laying off workers each of the last several years. Person-A has no experience building or using bombs or firearms. Among the courses Person-A took in university are courses in computer network administration and computer security. He took advantage of a student discount to take a ZYXCompany Computer Security Essentials course, which included hands-on instruction in the use of computer administrative tools which, while the course taught their use for legitimate purposes, could be used as part of a malicious cyber attack. Not willing to die in while conducting an attack, Person-A has come to the belief that a large cyber attack against some aspect of CountryA's critical infrastructure is his attack method of choice. For the last six months, Person-A has been using automated attack tools to conduct anonymous attacks against various corporate websites and computer networks. To date, Person-A's activities have been limited to Denial of Service, website defacements, and intrusions to explore and seek information about networks (but not destroy information). The sophistication of the tools Person-A uses has been steadily increasing, but he is reliant on tools created by others.

PERSON-B

Person-B is a member of Organization-A (please see Organization-A's vignette for further information about Organization-A). Person-B grew up in CountryA and attended a public university there, graduating with an undergraduate degree in Chemistry with a minor in Computer Science one year ago. Person-B is a fairly recent religious convert, converting three years ago while in University. During his conversion process, Person-B met a small group of individuals who quickly became new friends. This group all believed in the extremist religious ideology of Organization-A, with two of the individuals being members of Organization-A. Heavily influenced by his friends, Person-B's religious conversion included the adoption of the same extremist religious beliefs. Organization-A, through his two friends who were members, recruited Person-B to join the organization six months ago. Person-B has been using his computer knowledge to enhance Organization-A's ability to communicate over the Internet in what they believe are more secure ways. Person-B also contributes to the production of propaganda and training materials, and helps a team of two others in maintaining Organization-A's website, web forum, and social media presences.

ORGANIZATION C

Organization-C is a CountryA-wide terrorist organization who first came into existence six years ago. The organization is politically motivated. Their principal concerns revolve around a specific industrial practice which they believe causes harm to the environment and human and animal health. Although there are non-members who also hold these concerns and engage in protest activity related to them, Organization-C engaged in violent actions intended to coerce industry to stop the practice, government to intervene to stop the practice, and supporters/supplies/customers of the Industry to pressure the Industry to stop the practice. Prior actions claimed by Organization-C include sabotage, arson, and bombings of Industry facilities. In the last two years, the level of violence has increased. In particular, while historically Organization-C has taken steps to ensure that people were not present during their attacks (such as by calling in an advance warning, or attacking facilities at night during non-operational hours), the last four bombings, occurring at approximately six month intervals, have been of Industry facilities during operational hours. The number of deaths have ranged from two to 25 and injuries over 100 with each bombing. Organization-C has also engaged in an escalating cyber campaign for all six years of their existence. Initially satisfied with website defacements, in the past three years the organization has claimed responsibility for numerous denial of service attacks. In addition, it is believed to be responsible for two Advanced Persistent Threat (APT)-type attacks in which they gained access to two corporate networks and exfiltrated sensitive corporate documents over a period lasting nine and 15 months respectively. Some of the exfiltrated documents were subsequently published on independent media websites, citing Organization-C as their source. Organization-C is believed to have two “cyber expert” groups which operate independently of each other but share training and transfer knowledge amongst each other. Each of these groups consist of between three and five young adults between the ages of 19 and 24 years old. Each person has experience with conducting various types of cyber attacks, and two are known to have completed computer science degrees which include coursework in programming, network security, and network administration. Member of the groups are known to frequent web forums and social media venues popular with hackers, and are believed to gain information about new hacking and other cyber attack techniques through these forums and the relationships they have cultivated with hackers who commit cyber crime for financial gain. Two months ago, a user believed to be a member of one of these groups made a post to a hacker forum asking for tips on “taking down” critical infrastructure facilities. In the post, a US Government video available on the Internet was referenced. The video shows part of an experiment that was conducted where a cyber attack was used to overload an industrial generator, causing it to catch fire. One member of Organization-C’s “cyber experts” groups has a father who is a Vice President at one of the leading Industry companies, but who is unaware of his daughter’s affiliation with Organization-C.

PERSON-C (to be read in conjunction with the description of Organization-C)

Person-C is a twenty-one year old female residing in the Capital City of CountryA. Person-C believes strongly in the ideology and tactics used by Organization-C to advance its goals, and has been a member of the organization for just over three years. Ten months ago, Person-C moved from a position providing social media and communications support to join one of the organization's two "cyber expert" groups. Person-C is currently enrolled in the third year of a computer engineering undergraduate program. Person-C has been writing software programs, primarily for personal use, since Person-C was fourteen years old, and has engaged in hacking, first for personal enjoyment, but later in support of Organization-C's goals, since Person-C was sixteen years old. Person-C's father is a Vice President at CompanyA, one of the leading companies in the Industry Organization-C opposes. Person-C's father is not aware of his daughter's participation in Organization-C. Person-C has made public statements on a semi-anonymous social media website that Person-C believes Organization-C should do "whatever it takes" to stop the Industry and that since "time is running out", "more creative actions are required."

APPENDIX D

FINAL ANALYTICAL TOOL INSTRUMENT

INTRODUCTION TO THE TOOL

This structured analytical tool is used to assist analysts in assessing the level of cyber threat posed by terrorist entities and individuals¹ to CountryA.² It provides a structured way of assessing the threat, and in addition to an overall threat level, the tool is used to assist in the development of an assessment narrative to accompany the tool's result.

Threat is composed of two components: **intent** and **capability**. That is, the terrorist entity/individual's intent to carry out cyber attacks, and their capability to actually do so. For the purpose of this tool, "cyber attacks" are the use of cyber methods as a means to attack cyber targets (although a physical target (such as a physical system controlled by a computerized device) may be the ultimate intended target, "cyber attacks" are conducted through cyber rather than kinetic means against physical targets). The tool is NOT intended to examine computer-enabled crime nor other supportive use of information technologies where computers are not the method, means, and target of attack.

To assess intent and capability, a number of indicators of each have been identified. Each indicator is defined. Each indicator then has defined levels of "high", "medium", "low", "none", and "unknown". Within both categories of intent and capability, the indicators are divided into "Tier 1" and "Tier 2" indicators. The two tiers are used to help develop an overall level to assign to intent and to capability and reflect indicators that strongly contribute to the category level (Tier 1), and indicators that less strongly contribute (Tier 2). The overall levels of intent and capability are then compiled together to form the overall threat level of the assessment.

HOW TO USE THE TOOL: GENERAL INFORMATION

The tool is not intended to be used as a stand-alone assessment. In addition to providing a picture of the overall cyber threat level, the tool is an aid to judgement – it is used to assist in the development of an accompanying assessment narrative. This overall assessment is based on the information available at the time it is conducted, with the narrative is used to qualify, provide context, and state the analytical judgements. A more detailed discussion of the narrative follows in the next section.

Each terrorist entity or individual is assessed individually. Once assessed, groups and individuals may be compared to each other, or compared to themselves over a period of time.

¹ "terrorist entities and individuals" refer to entities and individuals who meet the definition of "terrorist group" or similar designation under the criminal laws of the country making use of the tool and similarly motivated entities/individuals who act within the cyber realm.

² "CountryA" is used as a placeholder for the reference country. In actual use, the country of concern (e.g. Canada, United States, United Kingdom) would be used in place of "CountryA".

The tool is worded to assess a general cyber threat. However, it is possible to specify a specific type of cyber threat, a specific target (e.g. by company, location, type of asset, specific device as a target, etc), a specific time horizon, or a different country or more specific location, by adding the appropriate words to the appropriate indicators. When writing an assessment using this tool, an indication of this type of specificity should be included.

HOW TO USE THE TOOL: ASSESSMENT NARRATIVE

The accompanying narrative is an essential element when using the tool. The narrative states the analytical judgements, drawn from the Tool's built-in worksheet. It provides context to understand those judgements. It describes and qualifies the information used to conduct the assessment, explains its source(s), and speaks to its reliability and validity. The narrative includes illustrative examples and explanations or justifications for why indicators were judged at the level they were, including the thresholds used for specific indicators. It gives the rationale for assumptions that were made, and it highlights alternative judgements if those assumptions are incorrect. It explains situations where contradictory information gives rise to the insufficient information for assessment and thus an "unknown". It identifies intelligence gaps, and identifies opportunities to fill those gaps and strengthen knowledge in other areas.

The supporting narrative must discuss the "unknowns" and the intelligence gaps they represent. If there are sufficient unknowns, this aspect of the entity/individual becomes an intelligence requirement.

Narrative Examples (fictional)

Cyber attack history: HIGH. In January 2014, GroupX conducted two sophisticated cyber attacks against multiple well-protected government and private sector targets in Country A. Although the attacks were intended to cause disruption of critical infrastructure such as power outages and widespread government computer system failures, the results of the actual attacks were more limited in scope, causing... The sophisticated methods and tools used included...

Degree of Harm: HIGH. In December 2013 and again in February and March 2014, the senior leadership of GroupZ again encouraged their cyber corps to focus on attacks which results in loss of life instead of attacks to support fundraising that some members of the corps had been advocating. One attack was attempted in April 2014, targeting the traffic light control system of CityX. While the intent of the attack was to cause numerous fatal traffic accidents, the attack was unsuccessful.

External Sponsorship: LOW. In 2013, GroupV received US\$3,000 from CountryY to support its cyber corps. GroupV used the funds to purchase a new laptop computer from XYZCorp.

This tool can be used by an analyst alone or a group of subject matter experts.

To use the tool:

1. Identify the terrorist entity or individual to assess;
2. Assess a level (high, medium, low, none, unknown) for each indicator, as it applies to the terrorist entity/individual;
3. Determine the overall level for each of INTENT and CAPABILITY, documenting supporting evidence in the worksheet (Annex A), using the following rules:
 - a. The overall level is the highest level indicated by either of:
 - i. ONE Tier 1 indicator; or
 - ii. TWO Tier 2 indicators
 - b. Analytical judgement must be used to determine appropriate thresholds for some indicators (the threshold used should be explained in the narrative).
4. Using the overall levels for INTENT and CAPABILITY, select the appropriate overall threat level from the Threat Level Table. Annex B provides an example illustrating how individual indicator scores influence overall intent and capability levels, which in turn inform the overall threat level.
5. A supporting narrative should accompany any assessment using this tool.

INDICATORS

Each indicator is arranged using the following outline, consisting of an indicator name, its definition, and defined levels:

| | | |
|-----------------------|--------------------------|-------------------------------------|
| INDICATOR NAME | Definition of indicator. | |
| | UNKNOWN | Unable to assess. |
| | NONE | Definition of none for indicator. |
| | LOW | Definition of low for indicator. |
| | MEDIUM | Definition of medium for indicator. |
| | HIGH | Definition of high for indicator. |

INTENT INDICATORS – TIER ONE

| | | |
|---|--|---|
| CYBER ATTACK HISTORY | The extent to which cyber attacks have previously been committed against CountryA targets, including successful attacks, attempted attacks, foiled conspiracies, and non-criminal demonstrations of skill (such as formal cyber war-games). | |
| | UNKNOWN | Unable to assess. |
| | NONE | No demonstrated planning or use of cyber attacks against CountryA targets. |
| | LOW | Demonstrated planned use of cyber attacks against CountryA targets, but no attack attempted. |
| | MEDIUM | Demonstrated attempted use of cyber attacks against CountryA targets. |
| | HIGH | Demonstrated successful use of cyber attacks against CountryA targets. |
| STATED INTENT TO CONDUCT CYBER ATTACKS | The stated intent (publically or through confirmed private communications) to conduct cyber attacks against CountryA targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No stated intent to commit cyber attacks against CountryA targets. |
| | LOW | Has made public statements or threats to conduct cyber attacks against CountryA targets. |
| | MEDIUM | Has made internal statements proposing or discussing the desirability of cyber attacks against CountryA targets. |
| | HIGH | Has had internal discussions and conducting planning regarding conducting cyber attacks against CountryA targets. |

| | | |
|-----------------------|---|---|
| DEGREE OF HARM | The degree of cyber attack harm planned, attempted, or carried out against CountryA targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No harm against CountryA targets. |
| | LOW | Embarrassment or minor monetary or information losses against CountryA targets. |
| | MEDIUM | Physical damage including significant disruption to critical infrastructure (e.g. causing power outages) or significant monetary and information losses against CountryA targets. |
| | HIGH | Loss of human life or grave national reputational, economic or physical losses against CountryA targets. |

INTENT INDICATORS – TIER TWO

| | | |
|--|--|--|
| CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | The extent to which cyber attacks have previously been committed against non-CountryA targets, including successful attacks, attempted attacks, foiled conspiracies, and non-criminal demonstrations of skill (such as formal cyber war-games). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No demonstrated planning or use of cyber attacks against non-CountryA targets. |
| | LOW | Demonstrated planned use of cyber attacks against non-CountryA targets, but no attack attempted. |
| | MEDIUM | Demonstrated unsuccessful attempt to use of cyber attacks against non-CountryA targets. |
| | HIGH | Demonstrated successful use of cyber attacks against non-CountryA targets. |

| | | |
|--|---|--|
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | The extent to which the use of cyber attacks are encouraged or permitted by motivating ideology and supporting doctrine/normal operating procedures. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No support for cyber attacks in ideology and doctrine/normal operating procedures. |
| | LOW | Ideology supports use of cyber attacks, but there is no supporting doctrine/normal operating procedures for their use. |
| | MEDIUM | Doctrine/normal operating procedures supports some use of cyber attacks. |
| | HIGH | Doctrine/normal operating procedures strongly support and encourage use of cyber attacks. |

| | | |
|--|---|---|
| ACCEPTABLE USE OF CYBER ATTACKS | Situations in which cyber attacks may be used. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Cyber attacks are unacceptable. |
| | LOW | Cyber attacks are only to be used as a retaliatory tool. |
| | MEDIUM | Cyber attacks are an offensive tool only under limited circumstances. |
| | HIGH | Cyber attacks are an offensive tool under any circumstance. |

CAPABILITY INDICATORS – TIER ONE

| | | |
|----------------------------|---|--|
| TECHNICAL EXPERTISE | The extent of demonstrated technical expertise for conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No technical expertise. |
| | LOW | Some theoretical technical expertise but no or limited practical use of cyber attack methods. |
| | MEDIUM | Extensive theoretical expertise but no or limited practical use of cyber attack methods OR extensive practical use but limited theoretical knowledge. |
| | HIGH | Extensive theoretical knowledge AND extensive practical experience. |

| | | |
|-----------------------|---|---|
| SOPHISTICATION | The extent to which a sophisticated cyber attack can be carried out (includes resources needed). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No capability and no previous attacks. |
| | LOW | Demonstrated skills and resources to plan and carry out crude attacks. |
| | MEDIUM | Demonstrated skills and resources to plan and carry out sophisticated attacks, but no prior successful sophisticated attacks. |
| | HIGH | Demonstrated skills and resources to plan and carry out sophisticated attacks, and history of prior successful sophisticated attacks. |

| | | |
|-------------------|--|--|
| INNOVATION | Ability to innovate and independently develop new cyber attack methods and tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to use or develop new cyber attack methods and tools. |
| | LOW | Ability to use but not independently develop cyber attack methods and tools; reliant on methods and tools developed by others. |
| | MEDIUM | Ability to independently develop some cyber attack methods and tools, but dependent on others for most cyber attack methods and tools. |
| | HIGH | Ability to independently develop most or all cyber attack methods and tools required. |

CAPABILITY INDICATORS – TIER TWO

| | | |
|------------------------|---|--|
| HUMAN RESOURCES | Extent of human resources that are dedicated to cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No resources dedicated to cyber attacks. |
| | LOW | Only individual(s) working independently are dedicated to cyber attacks. |
| | MEDIUM | A single team of a few individuals is dedicated to cyber attacks. |
| | HIGH | A large single team or multiple teams are dedicated to cyber attacks. |

| | | |
|--|---|---|
| INFORMATION COLLECTION ON TARGET(S) | Methods for information gathering about prospective cyber target(s). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Conduct no information gathering about prospective targets. |
| | LOW | Basic information gathering, largely limited to public open source information. |
| | MEDIUM | Moderate information gathering, including use of social engineering methods. |
| | HIGH | Sophisticated information gathering, including multiple methods such as directed social engineering, and/or advanced persistent threat or other long term penetration and collection methods. |

| | | |
|---|--|--|
| ACCESS TO INSIDER INFORMATION ON TARGET(S) | Extent of infiltration of target (directly or through corruption or recruiting or coercion of employees) to gain insider-level information. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | None. |
| | LOW | No demonstrated history of infiltration of targets in any capacity, but some prior attempts or plans to do so. |
| | MEDIUM | Demonstrated history of infiltration of targets in a non-technical capacity. |
| | HIGH | Demonstrated history of infiltration of targets in a technical capacity. |

| | | |
|---------------------|--|--|
| TARGET SCOPE | Ability to conduct sophisticated multiple simultaneous or sequential cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to conduct multiple simultaneous or sequential cyber attacks. |
| | LOW | Ability to conduct a limited number of multiple simultaneous or sequential cyber attacks. |
| | MEDIUM | Ability to conduct multiple simultaneous or sequential cyber attacks against a limited number different types of multiple targets. |
| | HIGH | Ability to conduct multiple simultaneous or sequential cyber attacks against as many targets of different types as desired. |

| | | |
|---|--|--|
| COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | Extent of collaboration with others conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No collaboration. |
| | LOW | Some collaboration with others, but no known exchange of information regarding cyber attack training, tools, and best practices. |
| | MEDIUM | Some collaboration, including limited exchange of information regarding cyber attack training, tools, and best practices. |
| | HIGH | Strong collaboration, including extensive exchange of information regarding cyber attack training, tools, and/or best practices. |

| | | |
|-----------------------------|--|--|
| EXTERNAL SPONSORSHIP | Sources of resource sponsorships, including finances and/or cyber attack training and/or tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No external sponsorship. |
| | LOW | Sponsor provides limited resources. |
| | MEDIUM | Sponsor provides moderate resources. |
| | HIGH | Sponsor provides extensive resources. |

ASSESSMENT TABLE – OVERALL SUMMARY

| (Name of terrorist entity/individual being assessed) | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL INTENT | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER ONE | | | | | |
| CYBER ATTACK HISTORY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| STATED INTENT TO CONDUCT CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| DEGREE OF HARM | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER TWO | | | | | |
| CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ACCEPTABLE USE OF CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

| (Name of terrorist entity/individual being assessed) | | | | | |
|--|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL CAPABILITY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 1 | | | | | |
| TECHNICAL EXPERTISE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| SOPHISTICATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INNOVATION | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 2 | | | | | |
| HUMAN RESOURCES | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INFORMATION COLLECTION ON TARGET(S) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ACCESS TO INSIDER INFORMATION ON TARGET(S) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET SCOPE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| EXTERNAL SPONSORSHIP | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

THREAT LEVEL TABLE

Using the following table, plot the overall level for each of INTENT and CAPABILITY to determine the overall assessment threat level.

| | | CAPABILITY | | | |
|--------|--------|------------|----------|----------|-----------|
| | | NONE | LOW | MEDIUM | HIGH |
| INTENT | NONE | NONE | VERY LOW | VERY LOW | LOW |
| | LOW | VERY LOW | LOW | LOW | MEDIUM |
| | MEDIUM | LOW | MEDIUM | MEDIUM | HIGH |
| | HIGH | LOW | MEDIUM | HIGH | VERY HIGH |

Unknowns represent intelligence gaps. Analytical judgement determines when the group/individual as a whole represents an intelligence gap that cannot be assessed. This table cannot be used if either intent or capability are assessed as unknown. In such a case, the assessment itself must be used to clearly state the level that is known and that the other is unknown.

While it is more difficult to establish or change capabilities than intent, intent has stronger influence over the overall level; it is a necessary but not sufficient measure.

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

INTENT INDICATORS – TIER ONE

| | | |
|-----------------------------|---|--|
| CYBER ATTACK HISTORY | The extent to which cyber attacks have previously been committed against CountryA targets, including successful attacks, attempted attacks, foiled conspiracies, and non-criminal demonstrations of skill (such as formal cyber wargames). | |
| | UNKNOWN | Unable to assess. |
| | NONE | No demonstrated planning or use of cyber attacks against CountryA targets. |
| | LOW | Demonstrated planned use of cyber attacks against CountryA targets, but no attack attempted. |
| | MEDIUM | Demonstrated attempted use of cyber attacks against CountryA targets. |
| | HIGH | Demonstrated successful use of cyber attacks against CountryA targets. |

FACTING: CYBER ATTACK HISTORY

| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
|---|------------------------------------|-------------------|---------------------------|
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |

ASSESSMENT & NARRATIVE: CYBER ATTACK HISTORY

Overall assessment of indicator level (unknown, none, low, medium, high):

Supporting Narrative:

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

INTENT INDICATORS – TIER ONE

| | | |
|---|--|---|
| STATED INTENT TO CONDUCT CYBER ATTACKS | The stated intent (publically or through confirmed private communications) to conduct cyber attacks against CountryA targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No stated intent to commit cyber attacks against CountryA targets. |
| | LOW | Has made public statements or threats to conduct cyber attacks against CountryA targets. |
| | MEDIUM | Has made internal statements proposing or discussing the desirability of cyber attacks against CountryA targets. |
| | HIGH | Has had internal discussions and conducting planning regarding conducting cyber attacks against CountryA targets. |

| FACTING: STATED INTENT TO CONDUCT CYBER ATTACKS | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |

| ASSESSMENT & NARRATIVE: STATED INTENT TO CONDUCT CYBER ATTACKS |
|---|
| Overall assessment of indicator level (unknown, none, low, medium, high): |
| Supporting Narrative: |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

INTENT INDICATORS – TIER ONE

| | | |
|-----------------------|---|--|
| DEGREE OF HARM | The degree of cyber attack harm planned, attempted, or carried out against CountryA targets. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No harm against Country A targets. |
| | LOW | Embarrassment or minor monetary or information losses against Country A targets. |
| | MEDIUM | Physical damage including significant disruption to critical infrastructure (e.g. causing power outages) or significant monetary and information losses against Country A targets. |
| | HIGH | Loss of human life or grave national reputational, economic or physical losses against Country A targets. |

| FACTING: DEGREE OF HARM | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: DEGREE OF HARM | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

INTENT INDICATORS – TIER TWO

| | | |
|--|---|--|
| CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | The extent to which cyber attacks have previously been committed against non-CountryA targets, including successful attacks, attempted attacks, foiled conspiracies, and non-criminal demonstrations of skill (such as formal cyber wargames). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No demonstrated planning or use of cyber attacks against non-CountryA targets. |
| | LOW | Demonstrated planned use of cyber attacks against non-CountryA targets, but no attack attempted. |
| | MEDIUM | Demonstrated unsuccessful attempt to use of cyber attacks against non-CountryA targets. |
| | HIGH | Demonstrated successful use of cyber attacks against non-CountryA targets. |

| FACTING: CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

INTENT INDICATORS – TIER TWO

| | | |
|--|---|--|
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | The extent to which the use of cyber attacks are encouraged or permitted by motivating ideology and supporting doctrine/normal operating procedures. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No support for cyber attacks in ideology and doctrine/normal operating procedures. |
| | LOW | Ideology supports use of cyber attacks, but there is no supporting doctrine/normal operating procedures for their use. |
| | MEDIUM | Doctrine/normal operating procedures supports some use of cyber attacks. |
| | HIGH | Doctrine/normal operating procedures strongly support and encourage use of cyber attacks. |

| FACTING: IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | | | |
|--|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

INTENT INDICATORS – TIER TWO

| | | |
|--|---|---|
| ACCEPTABLE USE OF CYBER ATTACKS | Situations in which cyber attacks may be used. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Cyber attacks are unacceptable. |
| | LOW | Cyber attacks are only to be used as a retaliatory tool. |
| | MEDIUM | Cyber attacks are an offensive tool only under limited circumstances. |
| | HIGH | Cyber attacks are an offensive tool under any circumstance. |

| FACTING: ACCEPTABLE USE OF CYBER ATTACKS | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: ACCEPTABLE USE OF CYBER ATTACKS | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER ONE

| | | |
|----------------------------|---|--|
| TECHNICAL EXPERTISE | The extent of demonstrated technical expertise for conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No technical expertise. |
| | LOW | Some theoretical technical expertise but no or limited practical use of cyber attack methods. |
| | MEDIUM | Extensive theoretical expertise but no or limited practical use of cyber attack methods OR extensive practical use but limited theoretical knowledge. |
| | HIGH | Extensive theoretical knowledge AND extensive practical experience. |

| FACTING: TECHNICAL EXPERTISE | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: TECHNICAL EXPERTISE | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER ONE

| | | |
|-----------------------|---|---|
| SOPHISTICATION | The extent to which a sophisticated cyber attack can be carried out (includes resources needed). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No capability and no previous attacks. |
| | LOW | Demonstrated skills and resources to plan and carry out crude attacks. |
| | MEDIUM | Demonstrated skills and resources to plan and carry out sophisticated attacks, but no prior successful sophisticated attacks. |
| | HIGH | Demonstrated skills and resources to plan and carry out sophisticated attacks, and history of prior successful sophisticated attacks. |

| FACTING: SOPHISTICATION | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: SOPHISTICATION | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER ONE

| | | |
|-------------------|--|--|
| INNOVATION | Ability to innovate and independently develop new cyber attack methods and tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to use or develop new cyber attack methods and tools. |
| | LOW | Ability to use but not independently develop cyber attack methods and tools; reliant on methods and tools developed by others. |
| | MEDIUM | Ability to independently develop some cyber attack methods and tools, but dependent on others for most cyber attack methods and tools. |
| | HIGH | Ability to independently develop most or all cyber attack methods and tools required. |

| FACTING: INNOVATION | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: INNOVATION | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER TWO

| | | |
|------------------------|---|--|
| HUMAN RESOURCES | Extent of human resources that are dedicated to cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No resources dedicated to cyber attacks. |
| | LOW | Only individual(s) working independently are dedicated to cyber attacks. |
| | MEDIUM | A single team of a few individuals is dedicated to cyber attacks. |
| | HIGH | A large single team or multiple teams are dedicated to cyber attacks. |

| FACTING: HUMAN RESOURCES | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: HUMAN RESOURCES | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER TWO

| | | |
|--|---|---|
| INFORMATION COLLECTION ON TARGET(S) | Methods for information gathering about prospective cyber target(s). | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | Conduct no information gathering about prospective targets. |
| | LOW | Basic information gathering, largely limited to public open source information. |
| | MEDIUM | Moderate information gathering, including use of social engineering methods. |
| | HIGH | Sophisticated information gathering, including multiple methods such as directed social engineering, and/or advanced persistent threat or other long term penetration and collection methods. |

| FACTING: INFORMATION COLLECTION ON TARGET(S) | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: INFORMATION COLLECTION ON TARGET(S) | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER TWO

| | | |
|---|--|--|
| ACCESS TO INSIDER INFORMATION ON TARGET(S) | Extent of infiltration of target (directly or through corruption or recruiting or coercion of employees) to gain insider-level information. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | None. |
| | LOW | No demonstrated history of infiltration of targets in any capacity, but some prior attempts or plans to do so. |
| | MEDIUM | Demonstrated history of infiltration of targets in a non-technical capacity. |
| | HIGH | Demonstrated history of infiltration of targets in a technical capacity. |

| FACTING: ACCESS TO INSIDER INFORMATION ON TARGET(S) | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: ACCESS TO INSIDER INFORMATION ON TARGET(S) | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER TWO

| | | |
|---------------------|--|--|
| TARGET SCOPE | Ability to conduct sophisticated multiple simultaneous or sequential cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No ability to conduct multiple simultaneous or sequential cyber attacks. |
| | LOW | Ability to conduct a limited number of multiple simultaneous or sequential cyber attacks. |
| | MEDIUM | Ability to conduct multiple simultaneous or sequential cyber attacks against a limited number different types of multiple targets. |
| | HIGH | Ability to conduct multiple simultaneous or sequential cyber attacks against as many targets of different types as desired. |

| FACTING: TARGET SCOPE | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: TARGET SCOPE | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER TWO

| | | |
|---|--|--|
| COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | Extent of collaboration with others conducting cyber attacks. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No collaboration. |
| | LOW | Some collaboration with others, but no known exchange of information regarding cyber attack training, tools, and best practices. |
| | MEDIUM | Some collaboration, including limited exchange of information regarding cyber attack training, tools, and best practices. |
| | HIGH | Strong collaboration, including extensive exchange of information regarding cyber attack training, tools, and/or best practices. |

| FACTING: COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX A: INDICATORS WORKSHEET

| | |
|------------------------------------|--|
| Terrorist Entity/Individual | |
|------------------------------------|--|

CAPABILITY INDICATORS – TIER TWO

| | | |
|-----------------------------|--|--|
| EXTERNAL SPONSORSHIP | Sources of resource sponsorships, including finances and/or cyber attack training and/or tools. | |
| | UNKNOWN | Insufficient information for assessment. |
| | NONE | No external sponsorship. |
| | LOW | Sponsor provides limited resources. |
| | MEDIUM | Sponsor provides moderate resources. |
| | HIGH | Sponsor provides extensive resources. |

| FACTING: EXTERNAL SPONSORSHIP | | | |
|---|------------------------------------|-------------------|---------------------------|
| Supporting evidence (description, summary) | Strength (reliability/validity) | Source of info | Classification of Info |
| (add additional lines as required) | | | |
| | | | |
| | | | |
| | | | |
| ASSESSMENT & NARRATIVE: EXTERNAL SPONSORSHIP | | | |
| Overall assessment of indicator level (unknown, none, low, medium, high): | | | |
| Supporting Narrative: | | | |

ANNEX B: EXAMPLE ASSESSMENT TABLE

ASSESSMENT TABLE – OVERALL SUMMARY

| FICTITIOUS TERRORIST ORGANIZATION Z | | | | | |
|---|--------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL INTENT | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| INTENT – TIER ONE | | | | | |
| CYBER ATTACK HISTORY | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| STATED INTENT TO CONDUCT CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| DEGREE OF HARM | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INTENT – TIER TWO | | | | | |
| CYBER ATTACK HISTORY (NON-COUNTRYA TARGETS) | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| IDEOLOGICAL AND DOCTRINAL SUPPORT FOR CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| ACCEPTABLE USE OF CYBER ATTACKS | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

(continued)

ANNEX B: EXAMPLE ASSESSMENT TABLE

| FICTITIOUS TERRORIST ORGANIZATION Z | | | | | |
|--|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| INDICATORS | unknown | none | low | medium | high |
| OVERALL CAPABILITY | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 1 | | | | | |
| TECHNICAL EXPERTISE | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| SOPHISTICATION | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INNOVATION | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| CAPABILITY – TIER 2 | | | | | |
| HUMAN RESOURCES | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| INFORMATION COLLECTION ON TARGET(S) | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ACCESS TO INSIDER INFORMATION ON TARGET(S) | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| TARGET SCOPE | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| COLLABORATION WITH OTHERS CONDUCTING CYBER ATTACKS | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| EXTERNAL SPONSORSHIP | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

THREAT LEVEL TABLE

| | | CAPABILITY | | | |
|--------|--------|------------|----------|----------|-----------|
| | | NONE | LOW | MEDIUM | HIGH |
| INTENT | NONE | NONE | VERY LOW | VERY LOW | LOW |
| | LOW | VERY LOW | LOW | LOW | MEDIUM |
| | MEDIUM | LOW | MEDIUM | MEDIUM | HIGH |
| | HIGH | LOW | MEDIUM | HIGH | VERY HIGH |

REFERENCES

- Institute for Intergovernmental Research. (2014). Retrieved from Nationwide SAR Initiative (NSI):
<http://nsi.ncirc.gov>
- Atzmüller, C., & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences*, 128-138.
- Barter, C., & Renold, E. (1999). The Use of Vignettes in Qualitative Research. *Social Research Update*. Retrieved from <http://sru.soc.surrey.ac.uk/SRU25.html>
- Bjelopera, J. P. (2013). *American Jihadist Terrorism: Combating a Complex Threat*. Washington: Congressional Research Service.
- Bloom, M. (2005). *Dying to kill: The allure of suicide terror*. New York: Columbia University Press.
- Bonneuil, N., & Auriat, N. (2000). Fifty years of ethnic conflict and cohesion: 1945–1994. *Journal of Peace*, 563–581.
- Braithwaite, A., & Li, Q. (2007). Transnational terrorism hot spots: Identification and impact evaluation. *Conflict Management and Peace Science*, 281–296.
- Brickey, J. (2012). Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace. *CTC Sentinel*, pp. 4-6.
- Bureau of Justice Assistance. (2005). *Intelligence-Led Policing: The New Intelligence Architecture*. Washington: U.S. Department of Justice. Retrieved from <https://www.ncjrs.gov/pdffiles1/bja/210681.pdf>
- CBC News. (2005). Al-Qaeda flourishing on internet, intelligence officials warn.
- Chatagnier, J. T., Mintz, A., & Samban, Y. (2012). The Decision Calculus of Terrorist Leaders. *Perspectives on Terrorism*, 125-144.
- Clark, R. M. (2010). *Intelligence Analysis: A Target-Centric Approach*. Washington: CQ Press.
- Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What To Do About It*. New York: HarperCollins Publisher.
- Cope, N. (2004). Intelligence-led policing or policing-led intelligence. Integrating volume crime analysis into policing. *British Journal of Criminology*.

- Dolnik, A. (2007). *Understanding Terrorist Innovation: Technology, tactics and global trends*. London: Routledge.
- Dolnik, A. (2007). *Understanding Terrorist Tactics: Technology, tactics and global trends*. London: Routledge.
- DRDC CRTI. (2005). *Consolidated Risk Assessment*. Retrieved from http://www.crti.drdcrddc.gc.ca/en/priorities/risk_assessments/default.asp
- Dugan, L., LaFree, G., & Piquero, A. (2005). Testing a rational choice model of airline hijackings. *Criminology*, 1031–1065.
- Gill, P., Horgan, J., Hunter, S. T., & D. Cushenbery, L. (2013). Malevolent Creativity in Terrorist Organizations. *The Journal of Creative Behavior*, 125-151.
- Grabo, C. M. (2002). *Anticipating Surprise: Analysis for Strategic Warning*. Washington: Joint Military Intelligence College.
- Intelligence and Security Committee (UK). (2006). *Report into the London Terrorist Attacks on 7 July 2005*.
- Jackson, B., Baker, J., Chalk, P., Cragin, K., Parachini, J., & Trujillo, H. (2005). *Appetite for destruction: Organizational learning in terrorist groups and its implications for combating terrorism*. California: RAND.
- Krebs, V. E. (2002). Mapping Networks of Terrorist Cells. *CONNECTIONS*, 43-52.
- Mateski, M., Trevino, C. M., Veitch, C. K., Michalski, J., Harris, J. M., Maruoka, S., & Frye, J. (2012). *Cyber Threat Metrics*. Albuquerque: Sandia National Laboratories. Retrieved from <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-065.pdf>
- Midlarsky, M., Crenshaw, M., & Yoshida, F. (1980). Why violence spreads: The contagion of international terrorism. *International Studies Quarterly*, 262–298.
- Morgan, D. (2005). *Challenges encountered during law enforcement investigations of terrorist use of information technology*. Denton, TX: Thesis (M.S.)--University of North Texas.
- O'Brien, L. B. (2011). The Evolution of Terrorism Since 9/11. *FBI Law Rnforcement Bulletin*. Retrieved from FBI: <http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011/the-evolution-of-terrorism-since-9-11>

- Rasmussen, M., & Hafez, M. (2010). *Terrorist innovations in weapons of mass effect: Preconditions, causes and predictive indicators (Report No. ASCO 2010-019)*. The Defense Threat Reduction Agency. Retrieved from <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA556986>
- Ratcliffe, J. H., Sorg, E. T., & Rose, J. W. (2014). Intelligence-Led Policing in Honduras: Applying Sleipnir and Social Psychology to Understand Gang Proliferation. *J Police Crim Psych*. doi:DOI 10.1007/s11896-014-9143-4
- Rogers, E. M. (1982). Information exchange and technological innovation. In *The transfer and utilization of technical knowledge* (pp. 105-123).
- Royal Canadian Mounted Police. (2000). *Sleipnir: The long matrix for organized crime. An analytic technique for determining relative levels of threat posed by organized crime groups*.
- Spencer, C. O. (1996, Spring). Intelligence Analysis Under Pressure of Rapid Change: The Canadian Challenge. *Journal of Conflict Studies*. Retrieved from <http://journals.hil.unb.ca/index.php/JCS/article/viewFile/4525/5349>
- Strang, S. (2005). *Project SLEIPNIR: An analytical technique for operational priority setting*. Royal Canadian Mounted Police.
- Strang, S. J. (2005). Project Sleipnir: An analytical technique for operational priority setting. *International conference on intelligence analysis*. Ottawa: Office of the Assistant Director of Central Intelligence for Analysis and Production, Central Intelligence Agency.
- Technical Analysis Group, Institute for Security Technology Studies, Dartmouth College. (2004). *Examining the Cyber Capabilities of Islamic Terrorist Groups*. Retrieved from <http://www.ists.dartmouth.edu/library/164.pdf>
- United Kingdom Cabinet Office, Performance and Innovation Unit. (1999). *Encryption and law enforcement*. Retrieved from <http://www.fipr.org/polarch/piu.pdf>
- United Nations Office on Drugs and Crime (UNODC). (2011). *Organized Crime| Tools and Publications| Criminal Intelligence Manual for Analysts*. Retrieved from United Nations Office on Drugs and Crime: http://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf

Vos Fellman, P., & Wright, R. (2004). Modeling Terrorist Networks - Complex Systems at the Mid-Range.

The Intelligencer, Journal of U.S. Intelligence Studies.

Wason, K. D., Polonsky, M. J., & Hyman, M. R. (2002). Designing Vignette Studies in Marketing.

Australasian Marketing Journal (AMJ), 41–58.

Weimann, G. (2004). *www.terror.net: How Modern Terrorism Uses The Internet*. Washington: United

States Institute of Peace. Retrieved from <http://www.usip.org/sites/default/files/sr116.pdf>