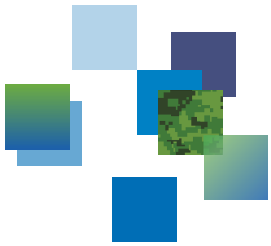
Defence Research and Development Canada
Recherche et développement pour la défense Canada

DRDC | RDDC



Ranking assets based on criticality and adversarial interest

Matthew Kellett
DRDC – Ottawa Research Centre

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2016-R168
August 2016

Canada

Ranking assets based on criticality and adversarial interest

Matthew Kellett
DRDC – Ottawa Research Centre

Defence Research and Development Canada
Scientific Report
DRDC-RDDC-2016-R168
August 2016

Abstract

We propose an approach to ranking computer network assets based on their criticality to an organization's current operations and business functions and their strategic importance to the organization's adversaries. An asset's criticality is a measure of its current importance to the organization, while an adversary's interest in the asset is a measure of its current importance to the adversary and, therefore, its future importance to the organization. We adapt techniques from existing work on asset criticality for use by a national defence organization. We also adapt these techniques to produce an adversarial interest score. We propose solutions for calculating these scores at the asset and the unit level and hybrid variants of both. We discuss options for combining asset criticality and adversarial interest scores to produce a list of assets or units ranked in order of their importance to the organization. The adversarial interest score can be used as an input to course-of-action recommendation algorithms. The combined ranked list of assets can be used by cyber defenders to prioritize the protection of assets within an organization.

Significance for defence and security

The techniques described in this report provide a way to introduce the knowledge of our adversaries' strategic goals and capabilities into the defence of our computer networks. The adversarial interest score for computer network assets can be used as an input to course-of-action recommendation algorithms, such as those proposed for the Automated Computer Network Defence (ARMOUR) technology demonstrator under the Cyber Decision Making and Response (CDMR) project. The combined ranked list of assets or units can be used to prioritize the protection of the most critical assets within our computer networks. By introducing adversarial interest into our view of which assets are most important, we provide a better defence of both our current operations and our future strategic advantage.

Résumé

Nous proposons une approche afin de classer les biens des réseaux informatiques en fonction de leur criticité par rapport aux activités en cours et aux fonctions opérationnelles d'une organisation, ainsi que de leur importance stratégique pour les adversaires de l'organisation. La criticité d'un bien est la mesure de son importance actuelle pour l'organisation, alors que l'intérêt d'un adversaire pour un bien est la mesure de l'importance qu'il lui accorde actuellement et, par conséquent, de son importance future pour l'organisation. Nous adaptons les techniques tirées de travaux existants sur la criticité des biens à leur utilisation par une organisation de défense nationale. Nous les adaptons également en vue de déterminer le niveau d'intérêt de l'adversaire. Nous proposons des solutions pour évaluer l'intérêt à l'endroit du bien et de l'unité, de même que des variantes hybrides de chacun d'eux. Nous discutons des possibilités de combiner la criticité du bien et le niveau d'intérêt de l'adversaire dans le but de produire une liste des biens ou des unités classés par ordre d'importance pour l'organisation. Le niveau d'intérêt de l'adversaire peut être utilisé comme complément aux algorithmes des options recommandées. Le classement combiné des biens peut être utilisé par la cyberdéfense afin d'établir l'ordre de priorité de leur protection au sein d'une organisation.

Importance pour la défense et la sécurité

Les techniques décrites dans le présent rapport permettent d'intégrer la connaissance des capacités et des objectifs stratégiques de nos adversaires à la défense de nos réseaux informatiques. Le niveau d'intérêt de l'adversaire pour les biens des réseaux informatiques peut être utilisé comme complément aux algorithmes des options recommandées, notamment ceux proposés pour le démonstrateur technologique de la défense automatisée des réseaux informatiques (ARMOUR) dans le cadre du projet Prise de décision et intervention en cybernétique (PDIC). Le classement combiné des biens ou des unités peut être utilisé pour établir l'ordre de priorité de la protection des biens les plus essentiels de nos réseaux informatiques. En intégrant l'intérêt de l'adversaire pour nos biens jugés les plus importants, nous nous assurons une meilleure défense dans nos activités en cours, ainsi qu'un futur avantage stratégique.

Table of contents

List of tables

Acknowledgements

I would like to thank Captain James Lindsay and Conan Moore for their helpful feedback in the development of the unit-level and hybrid methodologies. I would like to thank Captain Jason MacDonald for his help in determining the best criteria for capturing adversarial interest.

This page intentionally left blank.

1 Introduction

When defending a computer network, it quickly becomes obvious that some assets—desktop computers, servers, network equipment, printers, etc.—are more important than others and, therefore, require more attention. While it is necessary to patch the computer in the corner that has not been used for months, that computer should certainly not be the focus of effort during a crisis. We can easily conclude that the disused computer in the corner is not critical to the organization's business, but determining the criticality to the organization of other assets can be much less obvious. How does one value similar assets? In Section 1.1, we discuss a number of approaches proposed in the literature for determining the value of computer network assets and their criticality to the organization's business.

In a national defence organization, the computer networks not only support ongoing missions and business functions, they contain information of strategic importance to adversaries. The information that is most important to the organization's adversaries strategically may not be critical to the day-to-day work of the organization itself. The loss or compromise of that information may have little impact on current operations, but may have significant impact on the organization's ability to carry out future operations.

In this context, we believe that it is necessary to include a measure of the adversary's interest into the calculations of an asset's criticality in order to appreciate the asset's whole value, both present and future. In doing so, we must contend with the nature of the typical adversary of a national defence organization, namely that they are well funded and well resourced. Their attacks often take advantage of previously unknown vulnerabilities through what are commonly known as *zero day* exploits. Their attacks are often very difficult to detect. We must also contend with the organization's large and continuously changing internal cyber environment.

We propose a solution in Section 3 at the asset level that combines a measurement of asset criticality within the organization with the organization's knowledge of adversarial interest. The result is a list of cyber assets ranked in order of our need to defend them. Our solution builds on the asset criticality approach of Kim and Kang [1], which is designed to handle large multi-unit, multi-mission organizations. We introduce their solution in detail in Section 2.

We modify Kim and Kang's approach by explicitly defining the criticality criteria being evaluated for each asset. Our proposed criticality criteria allow each asset to be evaluated by 1) its value as a platform for work and as a means to access the network, 2) the value of its data, and 3) its value to others as a network resource. We also remove the application of dependencies among assets due to the likely difficulty in gathering and maintaining this type of information within a large organization. We replace the dependencies with more generalized dependency-related criteria at the asset and organizational levels. For adversarial interest, we specify separate criteria based on what the organization knows or suspects about their adversaries' strategic goals and capabilities. We apply similar techniques to those we use to calculate asset criticality to produce an adversarial interest score for each asset. To combine asset criticality and adversarial interest, we propose a number of approaches that can produce a ranked list of assets. A detailed example is given in Section 4 to demonstrate how the technique works.

Even asset-level information may be difficult to gather in the often fast-moving network environment of a large organization. In Section 5, we propose a simplified version of the technique from Section 3 that assesses the value of assets at the unit level. Each unit in the organization is asked to categorize their assets as critical, essential, and non-essential and then rate these categories as they would assets in the asset-level approach. These scores are combined using the same techniques as the asset-level approach and then combined with adversarial interest scores calculated at the unit level using a subset of the approaches proposed at the asset level. The result is a potentially less granular but more easily maintained rating of units rather than assets. A detailed example is given in Section 6 to demonstrate how the technique works.

Finally, it is possible that some units will be capable of providing detailed asset-level information and others may not. In Section 7, we discuss a hybrid approach that allows for this variation and produces either asset-level or unit-level results for use by the organization. We conclude in Section 8 with a discussion of the methodologies, the relation of this work to the larger concept of measuring risk, and the possibilities for future work.

The work in this report is a deliverable under the Cyber Security and Defence Metrics component of the Cyber Decision Making and Response (CDMR) project within Defence Research and Development Canada (DRDC)'s Cyber Operations Science and Technology Program. Both proposed methods for calculating asset adversarial interest scores can be used as input to the course-of-action recommendation algorithms used by the Automated Computer Network Defence (ARMOUR) component of CDMR. The proposed methods for calculating asset criticality scores and the combination of asset criticality and adversarial interest scores can be used as an input to asset valuation in the ARMOUR data model. The proposed method for calculating unit-level asset criticality, adversarial interest, and combined scores was developed after discussions with Directorate Information Management Engineering and Integration (DIMEI) in support of their Cyber Security and Defence Preparedness Assessment Capability (CSDPAC) project.

1.1 Related work

The problem of determining the value of a computer network's assets is not a new one. While looking at the replacement cost for an asset or the lost productivity cost due to an asset's loss is useful in a pure business context, the impact of the loss of an asset on ongoing operations, what could be referred to as the asset's *criticality*, would appear to be the most useful approach for a national defence organization.

There have been a number of papers that have approached the asset criticality problem from a mission impact assessment point of view. One of the earliest by Beaudoin from DRDC [2] maps the dependencies of resources in the network and uses the network map that this creates to calculate the potential impact on operations of the loss of any specific asset. The work of Grimaila from the U.S. Air Force Institute of Technology (AFIT) and Fortson from the U.S. Air Force Research Laboratory (AFRL) uses a similar approach but focuses on the information that an asset contains rather than the asset itself. In [3], Grimaila and Fortson along with Mills from AFIT extend their previous work to propose a way to automate what they call the Cyber Incident Mission Impact Assessment (CIMIA) methodology. Goodall, D'Amico, and Kopylec from Applied Visions, Inc. propose Camus [4], a method for automatically mapping cyber assets to missions and users. Camus uses network logs to tie users to specific resources on the network, and their attendant cyber assets, that are being used to support specific missions.

A more holistic and less mission-centric view of the dependencies within a computer network comes from the work of Sawilla from DRDC. He proposes in [5] a modification to the PageRank algorithm (the basis of Google's search engine) to determine the most valuable assets in the network. As with Google's search, the more an asset is depended upon, the higher its importance. This approach has the benefit of allowing for the use of automation since it relies on information that is inherent in the network, such as its topology, rather than information that is likely external, such as which missions are using which assets. Sawilla and Ou from Kansas State University extend this concept in [6] to incorporate known published vulnerabilities into an attack graph of the network that allows for the ranking of assets based on how open they are to attacks. This attack graph approach is the basis for the ARMOUR component of CDMR project.

There are other somewhat less directly applicable approaches to the problem of asset criticality. Beaver, Patton, and Potok from Oak Ridge National Laboratory (ORNL) propose in [7] a way of automatically judging the value of the information that a host contains. They use a document classification approach where they first develop a list of keywords that are indicative of important topics and then rank each host based on how frequently those keywords appear in its documents. Cam from the U.S. Army Research Laboratory (ARL) proposes in [8] an approach called PeerShield, a way of measuring the resilience, control effectiveness, and controllability of the network's assets. The author proposes a number of techniques for measuring these attributes and developing control structures within the network to enhance them.

The main focus of our work is on adversarial interest rather than asset criticality, so we looked for existing solutions that are easy to adapt without introducing unwanted complexities. We chose Kim and Kang's approach to asset valuation [1] because it is simple in terms of the input required and scalable in terms of the size of the organization at which our solution is targeted. In the next section, we describe Kim and Kang's approach and the tools they use to accomplish their goals.

2 Kim and Kang's approach

Kim and Kang approach the asset criticality problem in [1] by taking into account the hierarchical nature of the environment in which the assets are employed. They set out in [1, Section 3] the following goals for their solution:

1. "The criticality scores of the assets should reflect the relative criticality of the assets." The scores should indicate the magnitude of the criticality, not just a ranking of assets by criticality.

2. "The criticality scores need to be compatible with each other despite the fact that they are calculated by separate commands." The scores should be comparable across disparate parts of the organization.

3. "The criticality scores should provide near real-time calculations." Small scale changes in the inputs should not cause large scale recalculations of scores.

In order to fulfill these goals, the authors examine a large number of approaches to measuring criticality and settle on two multiple-attribute decision making (MADM) methods: simple additive weighting (SAW), and the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS). See [1, Section 4.2] for a detailed description and further references.

2.1 Simple Additive Weighting (SAW)

SAW, which is also known as the weighted sum method, is a straightforward method for comparing entities based on multiple attributes. See [1, Section 4.2] for Kim and Kang's full description of SAW.

To calculate asset criticality using SAW, the asset's score for each criterion being considered is multiplied by the weight assigned to that criterion and all the weighted scores are summed to get an asset score. The SAW asset score x_i^S for asset A_i is calculated using the following formula:

$$x_i^S = \sum_{j=1}^{m} w_j s_{ij}, \tag{1}$$

where m is the number of criteria, w_j is the weight given to criterion j, and s_{ij} is A_i's score for the jth criterion. A small example with 4 assets and 3 criteria is presented in Table 1.

As an example from Table 1, the SAW asset score for Asset A_1 is calculated as $x_1^S = (3 \cdot 0.2) + (2 \cdot 0.5) + (4 \cdot 0.3) = 2.8$.

Table 1: *Example calculation of asset scores using SAW.*

		Asset scores			
Criteria	w_j	A_1	A_2	A_3	A_4
Criterion 1	0.2	3	5	4	3
Criterion 2	0.5	2	1	3	1
Criterion 3	0.3	4	2	3	3
$x_i^S =$		**2.8**	**2.1**	**3.2**	**2.0**

2.2 Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)

TOPSIS is a more complicated method of comparing entities based on multiple attributes. See [1, Section 4.2] for Kim and Kang's full description. The m criteria scores for each asset are considered points in m-dimensional space. The assets' scores are determined by calculating their relative closeness to a hypothetical ideal solution.

Let A^+ be the hypothetical ideal solution or *zenith* and A^- be the hypothetical negative ideal or *nadir*. The zenith and nadir are calculated by taking the maximum and minimum score, respectively, for each criterion across all assets. The scores for each criterion are then weighted. Asset A_i's score x_i^T is determined by calculating its relative closeness the hypothetical ideal, which is given by the following formula:

$$x_i^T = \frac{D_i^-}{D_i^+ + D_i^-} \tag{2}$$

Table 2: *Example calculation of asset scores using TOPSIS.*

		Asset scores				**Ideals**	
Criteria	w	A_1	A_2	A_3	A_4	A^+	A^-
Criterion 1	0.2	3	5	4	3	5	3
Criterion 2	0.5	2	1	3	1	3	1
Criterion 3	0.3	4	2	3	3	4	2
		Weighted scores					
Criterion 1		0.6	1.0	0.8	0.6	1.0	0.6
Criterion 2		1.0	0.5	1.5	0.5	1.5	0.5
Criterion 3		1.2	0.6	0.9	0.9	1.2	0.6
$D_i^+ =$		0.64	1.17	0.36	1.12		
$D_i^- =$		0.78	0.40	1.06	0.30		
$x_i^T =$		**0.55**	**0.26**	**0.75**	**0.21**		

where D_i^+ and D_i^- are the Euclidean distances from the weighted criteria scores of asset A_i to the weighted scores of A^+ and A^-, respectively. A small example using the same assets and criteria as the SAW example is presented in Table 2.

As an example from Table 2, we calculate the asset score for Asset A_1. In this case, we are measuring the Euclidean distance from A_1 to both the zenith A^+ and the nadir A^- and then calculating the relative closeness a to the zenith.

$$w = (0.2, 0.5, 0.3) \tag{3}$$
$$A_1 = w(3, 2, 4) = (0.6, 1.0, 1.2) \tag{4}$$
$$A^+ = w(5, 3, 4) = (1.0, 1.5, 1.2) \tag{5}$$
$$A^- = w(3, 1, 2) = (0.6, 0.5, 0.6) \tag{6}$$
$$D_1^+ = \sqrt{(1.0 - 0.6)^2 + (1.5 - 1.0)^2 + (1.2 - 1.2)^2} = 0.64 \tag{7}$$
$$D_1^- = \sqrt{(0.6 - 0.6)^2 + (0.5 - 1.0)^2 + (0.6 - 1.2)^2} = 0.78 \tag{8}$$
$$x_1^T = \frac{D_1^-}{D_1^+ + D_1^-} = \frac{0.78}{0.64 + 0.78} = 0.55 \tag{9}$$

A relative closeness of 1.0 means that the asset's score matches the zenith and a relative closeness of 0.0 means the score matches the nadir. The utility of this approach is that it allows points that are equidistant from either the zenith or nadir to be distinguished.

2.3 Calculating asset criticality scores

Kim and Kang calculate asset criticality scores using the following method, the full description of which can be found in [1, Section 5]. They assume a number of units that each have assets that need to be scored. Note that they use the term "command" to refer to any atomic part of the organization that shares the same goal or mission. In their example in [1, Section 6], the commands are a top-level command, a submarine, a research facility, and a medical unit. We use the term "unit" throughout the rest of this report to refer to this concept.

Step 1

In Step 1, the units calculate the raw asset criticality scores for all their assets. Each unit scores each of its asset on a set of criteria. The authors do not specify what those criteria should be but make a point of noting that the criteria need not be the same across all units. The scores range from 1 to 5, but could use any scale. As a scoring example, we could establish a criterion for evaluating an asset based on how easy it is to replace, assigning 5 for a specialized piece of hardware like a disk array, and 1 for a commodity desktop computer.

Each unit then assigns weights to each of the criteria to reflect the criterion's importance to the unit. The weights range from 0 to 1 and all the weights sum to 1.

Finally, the asset's raw criticality score is calculated using the TOPSIS method.

The authors note that one of the problems with TOPSIS as originally proposed is that new inputs can change the values of the zenith and/or nadir hypothetical ideals thus requiring all criticality scores for assets within a unit to be recalculated. They avoid this problem by using a zenith and nadir based on the maximum and minimum allowable scores, respectively, rather than the current maximum and minimum scores, so that the zenith is scored 5 across all criteria and the nadir is scored 1.

Step 2

The asset criticality scores are updated to reflect the relative importance of each unit. The organization assigns weights to each criterion and scores each unit on them. As with assets, the authors do not suggest what the criteria should be for units. As a scoring example, we could evaluate each unit based on its contribution to ongoing missions, assigning 5 for the military unit carrying out the mission, 4 for that unit's logistical support unit, and 1 for the research unit developing new clothing.

The scores for each unit are then calculated using the SAW method and then these scores are normalized by dividing them by the maximum score across all units.

Each unit then multiplies its raw asset criticality scores from Step 1 by the normalized unit score to get a unit-adjusted asset criticality score.

Step 3

The asset criticality scores are updated to reflect dependencies between assets. For instance, if asset A_1 is relied upon 50% by asset A_3 and 70% by asset A_6 then its new asset score is $a_1 = \max\{a_1, (0.5 \cdot a_3), (0.7 \cdot a_6)\}$, where a_i is the unit-adjusted asset criticality score of asset A_i. In other words, an asset is as important as the most important asset that depends on it. For example, if we think of an operations officer using a file server for her files, that server should be rated just as highly as her desktop computer is.

Step 4

The authors propose using "value-sensitive factors," such as who is currently using the asset, to update the criticality scores. However, they propose this concept as future work and do not discuss it further in the paper.

In the next section, we discuss how we modify Kim and Kang's approach. For an example of how they apply their own method, see [1, Section 6]. For an example of how we apply our modified version, see Section 4.1 below.

3 Asset-level methodology

In this section, we propose an asset-level approach to calculating both asset criticality (in Section 3.1) and adversarial interest scores (in Section 3.2) and then combining the two scores (in Section 3.3). Although the adversarial interest score can be a useful input to decision making in and of itself, we believe that providing a combined list gives a better overall view of the relative importance of assets. We describe various ways that this combined list can be generated. In Section 4, we give a detailed example of how these techniques would work in practice, including step-by-step calculations. We propose a simplified unit-level version of the methodology in Section 5 and present a detailed example for it in Section 6. We propose hybrid approaches to combine the two in Section 7.

3.1 Calculating asset criticality scores

We present a modified version of Kim and Kang's approach [1] to calculating asset criticality scores in just two steps instead of their original four. We present just the modifications here. For a full description of their method, see Section 2.3. For a full example of the modified calculations, see Section 4.1. The result of this calculation is a baseline asset criticality score for every asset in the organization that has been adjusted for the relative importance of each unit to which the assets belong.

Step 1

In their Step 1, Kim and Kang use TOPSIS to calculate the *raw criticality scores* for each asset based on scores and weights determined by each unit. We keep the same approach; however, where they do not specify the criteria to be rated, we do.

We ask each unit to rate their assets based on the following three criteria:

- Importance of the asset
- Importance of the asset's data
- Importance of the asset to others

The *importance of the asset* is a measure of how important the asset is as a platform for work and accessing the network or simply as a piece of equipment. How important is the asset to the person using it? Could the person move to a similar asset with little interruption to their work? How hard would the asset be to replace? Is it a commodity personal computer or a specialized disk array?

The *importance of the asset's data* is a measure of how important the files on the asset are. How important, unique, or sensitive are the files? How hard would it be to replace them or recover them?

The *importance of the asset to others* is a measure of how important the network services provided by the asset are. How many users does it serve? How hard would it be to replace the services provided?

We claim that these criteria are completely descriptive of the importance of a computer or server as an asset in a computer network. However, these are not the only criteria or perhaps even the best criteria that provide a complete description. For instance, we note above that the "importance of the asset" criterion is a measure of both the importance of the asset as a platform for work or network access and the importance of the asset as a piece of equipment. Since the former interpretation applies mostly to desktop computers and the latter to servers, we have chosen not to distinguish between the two facets of meaning for this criterion. Nevertheless, more work could be done to further define these criteria or find another comparable set of criteria.

Since each unit is free to weight the criteria as suits their own mission, we believe that the criteria are also flexible enough to handle units with disparate missions. For instance, an information technology (IT) department might give the most weight to the importance of the asset to others, since its mission is to provide network services. A military operations centre might give the most weight to the importance of the asset, since the loss of an asset, even for a short time, may disrupt its mission. Finally, a research centre might give the most weight to the importance of the asset's data, since its mission is to produce intellectual property that is of strategic importance to future operations.

Step 2

In their Step 2, Kim and Kang use a *normalized unit modifier* based on SAW to adjust the raw criticality scores for each asset to reflect the relative importance of each unit to the organization's overall mission in a *unit-adjusted asset criticality score*. We keep the same approach, but like the last step, we specify the criteria to be used.

We propose the following criteria for the rating of each unit by the organization:

- Importance to mission
- Importance to other units

Unlike the previous criteria for assets, we cannot claim that these criteria are completely descriptive of the importance of a unit within an organization. Units are more nebulous entities compared to computer network assets, so we would expect completely descriptive criteria for units to vary depending on the overall mission of the organization. We believe the criteria as proposed here are sufficient for our example in Section 4 and likely are a good starting point for criteria that describe units within a national defence organization.

Unused steps

In their Step 3, Kim and Kang adjust the weights of assets based on the dependencies between assets. We eliminate this step because we cannot see a clear way, at this time, to implement this step in a scalable manner. While it might be possible to generate these dependencies and develop a theory of how to measure how much of an asset's function is provided by its dependency on another asset, there do not appear to be any obvious sources for quickly and reliably generating this information in the networks that we are likely to target with this methodology, especially when we include factors not inherent in the system, such as ongoing missions.

Instead of using dependencies, we have added the "importance of the asset to others" criterion at the asset level and "criticality to other units" criterion at the unit level to capture these relationships. While these dependency-based criteria are not as accurate as well-reasoned and well-maintained dependencies would be, we believe that in a less-than-ideal environment the scores assigned to these criteria will change less frequently and will therefore be inherently easier to maintain and likely more scalable.

In Step 4, Kim and Kang propose future work. We do not address any of their suggestions, but there are several related ideas that we discuss as possible follow-on work in Section 8.

In summary, we use Kim and Kang's approach from [1] as the basis of our approach to asset valuation for the purposes of this report. We modify their first step to specify criteria that capture the importance of an asset within its unit. We modify their second step to use criteria that we believe are a good starting point for scoring units (commands, units, agencies, establishments, etc.) within a national defence organization. Instead of specifying dependencies, as Kim and Kang do in their third step, we have included criteria that allow each asset and unit to be rated on how dependent others are on them. The result of this calculation is a unit-adjusted asset criticality score that is comparable across all units for every asset in the organization. We show all the steps of our calculations in our example in Section 4.

3.2 Calculating adversarial interest scores

We measure adversarial interest in much the same way that we measure asset criticality. We give each asset a score for a number of criteria. These criteria are then weighted. An *adversarial interest score* can then be calculated using either SAW or TOPSIS. This process is targeted at the organizational level—all assets are rated individually—so there is no need adjust the scores by unit.

We propose the following criteria to rate adversarial interest:

- Strategic importance
- Actor skill

The *strategic importance* of an asset is a measure of the degree to which the asset would further a known strategic goal of a specific adversary. For instance, if we know through reliable reporting that an adversary is extremely interested in our research on materials for cold-weather gloves, then the desktop computers and servers used to store the information on that research would be rated a 5 on a scale of 1 to 5. If an asset fits the known strategic goals of more than one adversary, the highest score is assigned.

The *actor skill* of an asset is a measure of how good the actors interested in that asset are likely to be. For instance, a crime syndicate that is going after social insurance numbers may rate a 2 for the computers that store those numbers, while a nation state going after glove research may rate a 5. If an asset is targeted by more than one adversary, the highest actor skill score is assigned.

In the absence of a way to validate the weighting of these two criteria, we suggest that an equal weighting, 0.5 each, is appropriate. We discuss approaches to validation in our discussion of potential future work in Section 8.

An adversarial interest score can then be calculated using SAW or TOPSIS. These scores can be used as input into a course of action recommendation algorithm or they can be used to produce a ranked list of assets.

3.3 Combining asset criticality and adversarial interest

Although the adversarial interest scores may be useful on their own, we believe that combining them with asset criticality scores produces a more meaningful output in the absence of further processing. The *combined asset score* allows for the generation of a ranked list of assets that reflects both the asset's importance to the organization and to its adversaries.

There are two obvious ways of combining the scores. If the adversarial interest score is calculated using SAW, then the weighted sums can be normalized and applied to the unit-adjusted asset criticality score. If it is calculated using TOPSIS, then the two scores can simply be averaged or they can be weighted and then averaged.

We show examples of all these combination methods in Section 4.3 and discuss their merits. Further work is required to determine the best approach. We discuss approaches to validation in Section 8.

4 Asset-level example

In this section, we present an example scenario to help illustrate our asset-level methodology and show the details. In our example, we have a national defence organization with five units: headquarters (HQ), a military unit (Mil), a corporate services section (CS), a research section (Res), and an information technology section (IT). The full list of assets for each unit is presented in Table 3. We describe the operational part of the scenario in Section 4.1 and the adversarial goals part in Section 4.2.

4.1 Calculating asset criticality scores

In our scenario, the headquarters has tasked the military unit with carrying out a mission. The command and control of the mission relies on the organization's computer network, which is run by the IT section. The corporate services section supports the other units by paying salaries, procuring equipment, and recruiting new employees, but it is not involved directly in the current mission. The research section is investigating cold weather clothing accessories, but the new technologies being developed will not be deployed in the field for 5–10 years.

We now show how the unit-adjusted asset criticality scores are calculated. In Table 4, we show the criteria weights and scores assigned to each asset by their unit. In Table 5, we show the criteria weights and scores assigned to each unit by the organization.

Let's use the Military Unit's Operations Officer's computer (Mil.OpsO), asset ID 7, to illustrate how we calculate its unit-adjusted asset criticality score. Let A_7 represent the computer as an asset.

The raw asset criticality score r_7 for A_7 is calculated using TOPSIS as follows:

$$w_M = (0.4, 0.4, 0.2) \tag{10}$$

$$A_7 = w_M(5, 5, 1) = (2.0, 2.0, 0.2) \tag{11}$$

$$A_M^+ = w_M(5, 5, 5) = (2.0, 2.0, 1.0) \tag{12}$$

$$A_M^- = w_M(1, 1, 1) = (0.4, 0.4, 0.2) \tag{13}$$

$$D_7^+ = \sqrt{(2.0 - 2.0)^2 + (2.0 - 2.0)^2 + (0.2 - 1.0)^2} = 0.8 \tag{14}$$

$$D_7^- = \sqrt{(2.0 - 0.4)^2 + (2.0 - 0.4)^2 + (0.2 - 0.2)^2} = 2.3 \tag{15}$$

$$r_7 = \frac{D_7^-}{D_7^+ + D_7^-} = \frac{2.3}{0.8 + 2.3} = 0.74 \tag{16}$$

Table 3: *Assets used in all examples.*

ID	Asset	Type	Description
Headquarters			
1	HQ.Comd	Desktop	Commander
2	HQ.COSOps	Desktop	Chief of Staff Operations
3	HQ.AA	Desktop	Administrative Assistant
4	HQ.Files	Server	File server
Military Unit			
5	Mil.CO	Desktop	Commanding Officer
6	Mil.Adj	Desktop	Adjutant
7	Mil.OpsO	Desktop	Operations Officer
8	Mil.SM	Desktop	Sergeant Major
9	Mil.Files	Server	File server
Corporate Services Section			
10	CS.Manager	Desktop	Manager
11	CS.Finance	Desktop	Finance
12	CS.Procure	Desktop	Procurement
13	CS.HR	Desktop	Human Resources
14	CS.Files	Server	File server
Research Section			
15	Res.Director	Desktop	Director
16	Res.SHats	Desktop	Scientist researching hats
17	Res.SGloves	Desktop	Scientist researching gloves
18	Res.SBoots	Desktop	Scientist researching boots
19	Res.Files	Server	File server
Information Technology Section			
20	IT.Analyst	Desktop	IT Analyst
21	IT.DC1	Server	Domain Controller 1
22	IT.DC2	Server	Domain Controller 2
23	IT.DNS1	Server	Domain Name Server 1
24	IT.DNS2	Server	Domain Name Server 2
25	IT.Mail	Server	Mail server

Table 4: *Criticality criteria weights and asset scores for asset-level example.*

	Importance		
	of Asset	**of Data**	**to Others**
HQ weights	0.5	0.3	0.2
HQ.Comd	4	4	1
HQ.COSOps	4	4	1
HQ.AA	1	3	2
HQ.Files	4	5	5
Mil weights (w_M)	0.4	0.4	0.2
Mil.CO	5	4	1
Mil.Adj	4	3	1
Mil.OpsO	5	4	1
Mil.SM	2	3	1
Mil.Files	5	4	4
CS weights	0.4	0.4	0.2
CS.Manager	3	4	1
CS.Finance	2	5	1
CS.Procure	2	4	1
CS.HR	2	3	1
CS.Files	2	5	5
Res weights	0.3	0.6	0.1
Res.Director	2	2	1
Res.SHats	2	4	1
Res.SGloves	2	4	1
Res.SBoots	2	4	1
Res.Files	2	5	5
IT weights	0.2	0.3	0.5
IT.Analyst	2	2	1
IT.DC1	5	5	4
IT.DC2	5	5	4
IT.DNS1	5	5	4
IT.DNS2	5	5	4
IT.Mail	4	4	5

Table 5: *Criteria weights and unit scores for all examples.*

	Importance	
	of Unit	**to Others**
Weights (w_C)	0.5	0.5
HQ	4	3
Mil	5	3
CS	2	1
Res	1	1
IT	5	5

where w_M represents the weights assigned by the Military Unit to each criterion for assessing assets (assume that it is transposed properly when multiplied against the asset criteria scores), A_7 represents the weighted scores assigned by the Military Unit to each asset criterion, and A_M^+ and A_M^- represent the zenith and nadir, respectively, after applying w_M.

Let $\mathcal{O}$ be the set of all units U_i within the organization. The normalized unit modifier u_M for the Military Unit U_M is calculated as follows:

$$w_U = (w_1, w_2) = (0.5, 0.5) \tag{17}$$

$$U_M = (s_1, s_2) = (5, 3) \tag{18}$$

$$x_M^S = \sum_{j=1}^{m} w_j s_j = 0.5 \cdot 5 + 0.5 \cdot 3 = 4.0 \tag{19}$$

$$u_M = \frac{x_M^S}{\max\limits_{i}^{\mathcal{O}} x_i^S} = \frac{4.0}{5.0} = 0.80 \tag{20}$$

where w_U represents the weights assigned by the organization to each criterion for assessing units, U_M represents the scores assigned by the organization to each unit criteria for the Military Unit, x_M^S is U_M's SAW score, $\max\limits_{i}^{\mathcal{O}} x_i^S$ is the maximum SAW score among all the units, and u_M is U_M's normalized unit modifier.

Finally, the unit-adjusted asset criticality score a_7 for A_7 is found by multiplying the raw asset criticality score r_7 by the normalized unit modifier u_M:

$$a_7 = r_7 \cdot u_M = 0.74 \cdot 0.80 = 0.59 \tag{21}$$

In Table 6, we show the unit-adjusted asset criticality scores (a_i) for all assets in our example in ranked order.

Table 6: *Ranking based on unit-adjusted asset criticality scores for asset-level example.*

Rank	**Asset**	a_i	**Rank**	**Asset**	a_i
1	IT.Mail	0.863	14	CS.Files	0.181
T2	IT.DC1	0.806	15	CS.Manager	0.164
T2	IT.DC2	0.806	16	CS.Finance	0.160
T2	IT.DNS1	0.806	17	HQ.AA	0.158
T2	IT.DNS2	0.806	18	Res.Files	0.146
6	Mil.Files	0.659	19	CS.Procure	0.137
7	HQ.Files	0.564	20	IT.Analyst	0.137
T8	Mil.CO	0.553	T21	Res.SHats	0.123
T8	Mil.OpsO	0.553	T21	Res.SGloves	0.123
T10	HQ.Comd	0.447	T21	Res.SBoots	0.123
T10	HQ.COSOps	0.447	24	CS.HR	0.105
12	Mil.Adj	0.437	25	Res.Director	0.049
13	Mil.SM	0.281			

4.2 Calculating adversarial interest scores

In our scenario, we have three reliable reports on adversaries whose strategic goals include the information stored on the organization's computer network.

The first adversary is a so-called "hacktivist" group that is looking for sensitive information to publicize or ways to simply disrupt the network, such as re-routing connections using the DNS server. They are considered most likely to attack the IT infrastructure and have a fairly low-level of sophistication.

The second adversary is a nation state that is known to have some interest in current military plans. They are considered likely to go after the military part of the organization, but, since they are not in active conflict with the organization's country, they are not considered likely to use their best cyber resources.

The third adversary is a nation state that is interested in moving militarily into a cold weather region; however, they lack the technology to effectively do so, especially gloves. They are considered likely to go after the research division, especially the work on gloves. They are likely to use their best cyber resources.

The process of turning these reports into numbers is not straightforward and needs to be based on an evaluation of the reports as a whole. We show one possible way of scoring based on these reports in Table 7 and use that scoring throughout the rest of the examples in this paper. For instance, for the first adversary, we assign 3 for strategic importance and 2 for actor ability to all assets in IT department. However, for the third adversary, we assign 5 for strategic importance and 5 for actor ability to the mail server (IT.Mail), because it may contain information related to our glove research, thus overwriting the values for the first adversary. For the second adversary, we assign 3 for strategic importance and 2 for actor ability to all assets in the Military Unit and the Headquarter's file server, but only 2 and 1, respectively, to the rest of the Headquarter's computers because they may only contain limited information on current plans.

A few things to note about how we have assigned scores. The goal in assessing adversarial interest is not accuracy so much as consistency. The resulting scores should reflect the relative differences among our adversaries' interests and among their abilities. We have chosen to only assess assets for which we have reliable reporting that the organization's adversaries have a direct interest. Since the corporate services section (CS) is not a known target, its assets are assigned default scores of 1. Another possible approach is to rank the adversaries based on their known attack methods. If one of the adversaries is known to use the potentially less-protected corporate services assets to gain a foothold in the network, we could change the scoring to reflect that.

As with asset criticality, let's use the Military Unit's Operations Officer's computer (Mil.OpsO) to illustrate how we calculate its adversarial interest score. We calculate adversarial interest using both SAW and TOPSIS. As with the previous example, let A_7 represent the asset. Let b_7^S represent its SAW adversarial interest score and b_7^T its TOPSIS adversarial interest score.

The SAW adversarial interest score is calculated as follows:

$$w_{\mathcal{O}} = (w_1, w_2) = (0.5, 0.5) \tag{22}$$

$$A_7 = (s_{71}, s_{72}) = (3, 2) \tag{23}$$

$$b_7^S = \sum_{j=1}^{m} w_j s_{7j} = 0.5 \cdot 3 + 0.5 \cdot 2 = 2.5 \tag{24}$$

where $w_{\mathcal{O}}$ represents the weights assigned by the organization to each criterion for assessing adversarial interest, and A_7 represents the scores assigned by the organization to each asset criteria.

Table 7: *Adversarial interest criteria weights and asset scores for asset-level example.*

	Strategic importance	**Actor skill**
Weights ($w_{\mathcal{O}}$)	0.5	0.5
HQ.Comd	2	1
HQ.COSOps	2	1
HQ.AA	2	1
HQ.Files	3	2
Mil.CO	3	2
Mil.Adj	3	2
Mil.OpsO	3	2
Mil.SM	3	2
Mil.Files	3	2
CS.Manager	1	1
CS.Finance	1	1
CS.Procure	1	1
CS.HR	1	1
CS.Files	1	1
Res.Director	3	3
Res.SHats	3	3
Res.SGloves	5	5
Res.SBoots	3	3
Res.Files	5	5
IT.Analyst	3	2
IT.DC1	3	2
IT.DC2	3	2
IT.DNS1	3	2
IT.DNS2	3	2
IT.Mail	5	5

The TOPSIS adversarial interest score is calculated as follows:

$$w_{\mathcal{O}} = (0.5, 0.5) \tag{25}$$
$$A_7 = w_{\mathcal{O}}(3, 2) = (1.5, 1.0) \tag{26}$$
$$A^+ = w_{\mathcal{O}}(5, 5) = (2.5, 2.5) \tag{27}$$
$$A^- = w_{\mathcal{O}}(1, 1) = (0.5, 0.5) \tag{28}$$
$$D_7^+ = \sqrt{(1.5 - 2.5)^2 + (1.0 - 2.5)^2} = 1.8 \tag{29}$$
$$D_7^- = \sqrt{(1.5 - 0.5)^2 + (1.0 - 0.5)^2} = 1.1 \tag{30}$$
$$b_7^T = \frac{D_7^-}{D_7^+ + D_7^-} = \frac{1.8}{1.1 + 1.8} = 0.38 \tag{31}$$

where $w_{\mathcal{O}}$ represents the weights assigned by the organization to each criterion for assessing adversarial interest (assume that it is transposed properly when multiplied against the adversarial interest scores), and A_7 represents the scores assigned by the organization to each of the asset's criteria.

In Table 8, we show the adversarial interest scores for all assets based on SAW (b_i^S) and TOPSIS (b_i^T). Unsurprisingly, both techniques result in the same ranking. Differences between the two techniques emerge when we use their attendant techniques in the next section to combine these adversarial interest scores with the unit-adjusted asset criticality scores we generated in the last section.

4.3 Combining asset criticality and adversarial interest scores

We now have two ranked lists of assets with scores. The asset criticality ranking in Table 6 is based on the unit-adjusted asset criticality scores calculated using our modification of Kim and Kang's approach from [1] (see Section 3.1). The adversarial interest ranking in Table 8 is based on adversarial interest scores calculated using both the SAW and TOPSIS techniques. In this section, we discuss a number of ways of combining asset scores and recommend, based on the example, the simple average of TOPSIS scores for asset criticality and adversarial interest.

Table 8: *Ranking based on SAW- and TOPSIS-calculated adversarial interest scores for asset-level example.*

Rank	**Asset**	b_i^S	b_i^T	**Rank**	**Asset**	b_i^S	b_i^T
T1	Res.SGloves	5.0	1.000	T7	IT.DC1	2.5	0.383
T1	Res.Files	5.0	1.000	T7	IT.DC2	2.5	0.383
T1	IT.Mail	5.0	1.000	T7	IT.DNS1	2.5	0.383
T4	Res.Director	3.0	0.500	T7	IT.DNS2	2.5	0.383
T4	Res.SBoots	3.0	0.500	T18	HQ.Comd	1.5	0.167
T4	Res.SHats	3.0	0.500	T18	HQ.COSOps	1.5	0.167
T7	HQ.Files	2.5	0.383	T18	HQ.AA	1.5	0.167
T7	Mil.CO	2.5	0.383	T21	CS.Manager	1.0	0.000
T7	Mil.Adj	2.5	0.383	T21	CS.Finance	1.0	0.000
T7	Mil.OpsO	2.5	0.383	T21	CS.Procure	1.0	0.000
T7	Mil.SM	2.5	0.383	T21	CS.HR	1.0	0.000
T7	Mil.Files	2.5	0.383	T21	CS.Files	1.0	0.000
T7	IT.Analyst	2.5	0.383				

For combining the asset criticality scores with the SAW adversarial interest scores, b_i^T, the obvious approach is to use the same normalization technique that is used for units when calculating unit-adjusted asset criticality scores. We normalize the SAW adversarial interest score and multiply it by the asset criticality score to get the result S_i^S. Let $\mathcal{A}$ be the set of all assets in the organization. Using Mil.OpsO, A_7, again as an example, we get the following calculation:

$$a_7 = 0.59 \tag{32}$$

$$b_7^S = 2.5 \tag{33}$$

$$S_7^S = a_i \cdot \frac{b_7^S}{\max\limits_{i}^{\mathcal{A}} b_i^S} = 0.59 \cdot \frac{2.5}{5.0} = 0.30 \tag{34}$$

For combining the asset criticality scores with the TOPSIS adversarial interest scores, b_i^T, the simplest approach is to take the average of the asset criticality score and the adversarial interest score to get the result S_i^T. Using A_7, we get the following calculation:

$$a_7 = 0.59 \tag{35}$$

$$b_7^T = 0.38 \tag{36}$$

$$S_7^T = \frac{a_7 + b_7^T}{1+1} = \frac{0.59 + 0.38}{2} = 0.49 \tag{37}$$

Another combination approach using the TOPSIS adversarial interest scores is to weight one of the inputs to the average higher than the other. We look at two scenarios: one that favours asset criticality scores, S_i^{T51}, which results from multiplying the asset criticality score by 5 and keeping the adversarial interest score untouched; and one that favours adversarial interest scores, S_i^{T15}, which does the opposite. The scores for A_7 are calculated as follows:

$$S_7^{T51} = \frac{(5 \cdot a_7) + b_7^T}{5+1} = \frac{(5 \cdot 0.59) + 0.38}{6} = 0.56 \tag{38}$$

$$S_7^{T15} = \frac{a_7 + (5 \cdot b_7^T)}{1+5} = \frac{0.59 + (5 \cdot 0.38)}{6} = 0.42 \tag{39}$$

Table 9 shows the base scores for each asset and the combined asset scores given by each combination technique and Table 10 shows the resulting ranking. Note that IT.DC1, IT.DC2, IT. DNS1, and IT.DNS2 share the same asset criticality and adversarial interest scores, so are always tied in the rankings. The same is true for Mil.CO and Mil.OpsO, and for Res.SBoots and Res.SHats.

The combining of the two lists (asset criticality and adversarial interest) is a balancing act between prioritizing assets that allow the organization to support current operations and protecting assets that support future operations. Each combination technique provides a combined list that promotes assets that are of adversarial interest and demotes assets that are not. In our example, S^S and S^{T51} produce similar results that are very close to the base asset criticality ranking. S^{T15} appears to give too much weight to adversarial interest by ranking Res.Files and Res.SGloves above the majority of the IT infrastructure.

Based on our example, we recommend the combined ranking provided by S^T, the simple averaging of TOPSIS-calculated asset criticality and adversarial interest scores. It appears to produce the most balanced ranking among all the combination techniques. For instance, Res.Files and Res.SGloves are moved into the top 10 and the corporate services section's asset are rated lowest in a reflection of their importance to our adversaries.

Table 9: *All calculated asset scores for asset-level example.*

Asset	a_i	b_i^S	b_i^T	S_i^S	S_i^T	S_i^{T51}	S_i^{T15}
HQ.Comd	0.447	1.5	0.167	0.134	0.307	0.400	0.213
HQ.COSOps	0.447	1.5	0.167	0.134	0.307	0.400	0.213
HQ.AA	0.158	1.5	0.167	0.047	0.162	0.159	0.165
HQ.Files	0.564	2.5	0.383	0.282	0.474	0.534	0.413
Mil.CO	0.553	2.5	0.383	0.276	0.468	0.524	0.411
Mil.Adj	0.437	2.5	0.383	0.218	0.410	0.428	0.392
Mil.OpsO	0.553	2.5	0.383	0.276	0.468	0.524	0.411
Mil.SM	0.281	2.5	0.383	0.141	0.332	0.298	0.366
Mil.Files	0.659	2.5	0.383	0.329	0.521	0.613	0.429
CS.Manager	0.164	1.0	0.000	0.033	0.082	0.136	0.027
CS.Finance	0.160	1.0	0.000	0.032	0.080	0.133	0.027
CS.Procure	0.137	1.0	0.000	0.027	0.069	0.115	0.023
CS.HR	0.105	1.0	0.000	0.021	0.053	0.088	0.018
CS.Files	0.181	1.0	0.000	0.036	0.091	0.151	0.030
Res.Director	0.049	3.0	0.500	0.030	0.275	0.124	0.425
Res.SHats	0.123	3.0	0.500	0.074	0.311	0.185	0.437
Res.SGloves	0.123	5.0	1.000	0.123	0.561	0.269	0.854
Res.SBoots	0.123	3.0	0.500	0.074	0.311	0.185	0.437
Res.Files	0.146	5.0	1.000	0.146	0.573	0.289	0.858
IT.Analyst	0.137	2.5	0.383	0.068	0.260	0.178	0.342
IT.DC1	0.806	2.5	0.383	0.403	0.595	0.736	0.453
IT.DC2	0.806	2.5	0.383	0.403	0.595	0.736	0.453
IT.DNS1	0.806	2.5	0.383	0.403	0.595	0.736	0.453
IT.DNS2	0.806	2.5	0.383	0.403	0.595	0.736	0.453
IT.Mail	0.863	5.0	1.000	0.863	0.932	0.886	0.977

Table 10: *Asset ranking based on combination techniques for asset-level example with Res.Files and Res.SGloves highlighted.*

Rank	**by** a_i	**by** S_i^S	**by** S_i^T	**by** S_i^{T51}	**by** S_i^{T15}
1	IT.Mail	IT.Mail	IT.Mail	IT.Mail	IT.Mail
2	IT.DC1	IT.DC1	IT.DC1	IT.DC1	Res.Files
3	IT.DC2	IT.DC2	IT.DC2	IT.DC2	Res.SGloves
4	IT.DNS1	IT.DNS1	IT.DNS1	IT.DNS1	IT.DC1
5	IT.DNS2	IT.DNS2	IT.DNS2	IT.DNS2	IT.DC2
6	Mil.Files	Mil.Files	Res.Files	Mil.Files	IT.DNS1
7	HQ.Files	HQ.Files	Res.SGloves	HQ.Files	IT.DNS2
8	Mil.CO	Mil.CO	Mil.Files	Mil.CO	Res.SHats
9	Mil.OpsO	Mil.OpsO	HQ.Files	Mil.OpsO	Res.SBoots
10	HQ.Comd	Mil.Adj	Mil.CO	Mil.Adj	Mil.Files
11	HQ.COSOps	Res.Files	Mil.OpsO	HQ.Comd	Res.Director
12	Mil.Adj	Mil.SM	Mil.Adj	HQ.COSOps	HQ.Files
13	Mil.SM	HQ.Comd	Mil.SM	Mil.SM	Mil.CO
14	CS.Files	HQ.COSOps	Res.SHats	Res.Files	Mil.OpsO
15	CS.Manager	Res.SGloves	Res.SBoots	Res.SGloves	Mil.Adj
16	CS.Finance	Res.SHats	HQ.Comd	Res.SHats	Mil.SM
17	HQ.AA	Res.SBoots	HQ.COSOps	Res.SBoots	IT.Analyst
18	Res.Files	IT.Analyst	Res.Director	IT.Analyst	HQ.Comd
19	CS.Procure	HQ.AA	IT.Analyst	HQ.AA	HQ.COSOps
20	IT.Analyst	CS.Files	HQ.AA	CS.Files	HQ.AA
21	Res.SHats	CS.Manager	CS.Files	CS.Manager	CS.Files
22	Res.SGloves	CS.Finance	CS.Manager	CS.Finance	CS.Manager
23	Res.SBoots	Res.Director	CS.Finance	Res.Director	CS.Finance
24	CS.HR	CS.Procure	CS.Procure	CS.Procure	CS.Procure
25	Res.Director	CS.HR	CS.HR	CS.HR	CS.HR

The determination of the best combination technique is ultimately subjective and may change over time based on how valuable the organization considers the assets that its adversaries are targeting. In Section 8, we propose potential future work for validating the combination methods and automating the scoring of both asset criticality and adversarial interest for assets.

5 Unit-level methodology

In this section, we propose a unit-level approach to calculating both asset criticality (in Section 5.1) and adversarial interest scores (in Section 5.2) and then combining the two scores (in Section 5.3). In the asset-level approach we propose in Section 3, one of the goals of our modifications to Kim and Kang's original approach [1] is to make our methodology as scalable as possible. We did this, in part, by specifying the same criteria across all assets and by removing the dependency step. Even with these simplifications, it may be difficult to find or generate the data needed to support that methodology, and that was indeed the case for DIMEI's CSDPAC project. The methodology we propose in this section should significantly reduce the effort required to generate and maintain the appropriate data. In Section 6, we present a detailed example of how the technique would work in practice, including step-by-step calculations.

5.1 Calculating asset criticality scores

In the asset-level methodology, each unit in the organization is required to identify and score each asset under its control and to maintain that rating over time. We propose a simple but significant modification to the asset-level methodology to allow the wholesale rating of assets at the unit level. While this approach is less granular and potentially less accurate than the asset-level approach, it should be easier to generate and maintain this information.

The unit is asked to identify assets in three categories: critical, essential, and non-essential. If the organization has definitions for these categories or has similar categories, they can be used instead. We say that an asset is critical if a temporary loss of the asset would significantly impact the unit's ability to carry out its mission. An asset is essential if a temporary loss of the asset would impact the unit's ability to carry out its mission. Finally, an asset is non-essential if a temporary loss of the asset would not significantly impact the unit's ability to carry out its mission. To make these categories compatible with each other and across the organization, the organization assigns a rating to each. For our example in Section 6, we use a rating of 4 for critical assets, 2 for essential, and 1 for non-essential. In other words, we consider critical assets twice as important as essential assets and 4 times as important as non-essential assets.

The unit-level raw asset criticality score is calculated using the asset categories instead of by individual asset. The unit first estimates or specifies the number or percentage of assets in each category. It then scores each asset category on a scale of 1 to 5 on the three asset criteria: importance of the asset, importance of the asset's data, and importance of the asset to others. The combined scores for the unit for each criterion are then calculated using the rating for each category assigned by the organization, the number or percentage of assets the unit has in each category, and the score assigned by the unit to each criterion. Using the combined scores for each asset criticality criterion, an initial asset criticality score for the unit is calculated using TOPSIS.

The rest of the methodology for calculating asset criticality remains the same. Each unit is scored across the organization and a normalized unit modifier is produced using the SAW technique. The final unit-adjusted asset criticality score for the unit is calculated by multiplying the unit's raw asset criticality score by the normalized unit modifier.

5.2 Calculating adversarial interest scores

The calculation of adversarial interest becomes much simpler in the unit-level methodology. While we can break up the assets into categories for determining the criticality of those assets to a unit, those categories may have little relation to the strategic goals of an adversary interested in a unit's assets. With that in mind and with the restriction of not being able to rate individual assets, the easiest and most effective way to express adversarial interest is to score the unit itself based on its most interesting assets. The unit-level adversarial interest score is calculated by having each unit scored on the two adversarial interest criteria: strategic importance, actor skill. The scores should be based on the maximum such scores for all "interesting" assets in the unit. The adversarial interest score is calculated for each unit using TOPSIS.

5.3 Combining asset criticality and adversarial interest

Finally, the unit-level asset criticality and adversarial interest scores are combined in the same way as the asset-level TOPSIS combination methodology, either by simple averaging in the basic case or by weighted averaging when fine tuning by operators is desired. The same fine tuning is not possible using the SAW methodology for computing the adversarial interest score, so we omit that as an option.

Even though this methodology produces a ranking among units, the result is still ultimately about the assets being protected. The units should be prepared to identify the assets in each category so that the mitigation of problems with critical assets can be prioritized over essential assets, which should be prioritized over non-essential. Similarly, assets that are of higher interest to adversaries should be identified and treated similarly to critical assets regardless of their asset category.

6 Unit-level example

We present an example calculation using the unit-level methodology and its accompanying formulas. For our example, we used the same 5 units as the asset-level example: a headquarters (HQ), a military unit (Mil), a corporate services section (CS), a research section (Res), and an information technology section (IT). We use the military unit (Mil) to show our example calculations. Because of the limited number of assets in the asset-level example, we use data that is similar to the asset-level example rather than exactly the same. We include only the calculations here.

6.1 Calculating asset criticality scores

In this section, we show how the unit-adjusted asset criticality scores are calculated for each unit based on their scoring of each category of assets. We start by calculating the raw asset criticality score for each unit. Table 11 shows the number or fraction of assets in each asset category for each unit, the weights assigned by each unit to the asset criteria, and the scores assigned by each unit to the asset criteria for each asset category. The organization has rated each asset category as 4 for critical, 2 for essential, 1 for non-essential.

The raw asset criticality score, r_M, for the Military Unit, M, is calculated as follows. The combined score for the importance-of-the-asset criterion, A_M^{Asset}, is the sum of the rating for each asset category times the number of assets in the asset category times the score for that asset category, all divided by the total number of assets weighted by the asset category ratings. The combined scores for the other criteria are calculated similarly.

$$A_M^{\text{Asset}} = \frac{(4 \cdot 9 \cdot 5) + (2 \cdot 6 \cdot 4) + (1 \cdot 0 \cdot 2)}{(4 \cdot 9) + (2 \cdot 6) + (1 \cdot 0)} = 4.5 \tag{40}$$

$$A_M^{\text{Data}} = 3.75 \tag{41}$$

$$A_M^{\text{Others}} = 1.75 \tag{42}$$

Table 11: *Criticality criteria weights and asset category size and scores for unit-level example.*

		Importance		
	Size	**of Asset**	**of Data**	**to Others**
HQ weights		0.5	0.3	0.2
Critical (4)	10	4	5	5
Essential (2)	20	4	4	1
Non-essential (1)	10	1	3	2
Mil weights		0.4	0.4	0.2
Critical	9	5	4	2
Essential	6	3	3	1
Non-essential	0	1	1	1
CS weights		0.4	0.4	0.2
Critical	0.1	2	5	5
Essential	0.2	2	3	1
Non-essential	0.7	1	1	1
Res weights		0.3	0.6	0.1
Critical	0	1	1	1
Essential	10	2	4	1
Non-essential	30	2	1	1
IT weights		0.2	0.3	0.5
Critical	20	5	5	4
Essential	5	1	1	3
Non-essential	2	2	2	2

The raw asset score r_M for the military unit M is calculated using TOPSIS as follows:

$$w_M = (0.5, 0.4, 0.1) \tag{43}$$
$$A_M = w_M(4.5, 3.75, 1.75) = (2.25, 1.5, 0.175) \tag{44}$$
$$A_M^+ = w_M(5, 5, 5) = (2.5, 2.0, 0.5) \tag{45}$$
$$A_M^- = w_M(1, 1, 1) = (0.5, 0.4, 0.1) \tag{46}$$
$$D_M^+ = \sqrt{(2.5 - 2.25)^2 + (2.0 - 1.5)^2 + (0.5 - 0.175)^2} = 0.84 \tag{47}$$
$$D_M^- = \sqrt{(0.5 - 2.25)^2 + (0.4 - 1.5)^2 + (0.1 - 0.175)^2} = 1.79 \tag{48}$$
$$r_M = \frac{D_M^-}{D_M^+ + D_M^-} = \frac{1.79}{0.84 + 1.79} = 0.68 \tag{49}$$

where w_M represents the weights assigned by the Military Unit to each asset criticality criterion (assume that it is transposed properly when multiplied against the asset criteria scores), A_M represents the weighted scores calculated from the scores assigned by the Military Unit for each asset category and asset criticality criterion, and A_M^+ and A_M^- represent the zenith and nadir, respectively, after applying w_M.

The normalized unit modifier u_i for all the units, including the military unit U_M is calculated using the unit scores from Table 5 and equations 17-20.

The unit-adjusted asset criticality score a_7 for A_7 is found by multiplying the raw asset criticality score r_7 by the normalized unit modifier u_M:

$$a_M = r_M \cdot u_M = 0.68 \cdot 0.7 = 0.54 \tag{50}$$

Table 12: *Adversarial interest criteria weights and asset scores for the unit-level example.*

	Strategic Importance	**Actor Skill**
Weights	0.5	0.5
HQ	3	2
Mil	3	2
CS	1	1
Res	5	4
IT	5	5

6.2 Calculating adversarial interest scores

Using essentially the same scenario, we now calculate adversarial interest scores for each unit as scored by the organization. As noted in the discussion on the unit-level methodology in the last section, the scores should be based on the assets within each unit that are of most interest to the organization's adversaries. Table 12 shows the weights and scores assigned by the organization to each unit for adversarial interest for our example.

The adversarial interest score is calculated using TOPSIS as follows:

$$w_{\mathcal{O}} = (0.5, 0.5) \tag{51}$$
$$A_M = w_{\mathcal{O}}(3, 2) = (1.5, 1) \tag{52}$$
$$A^+ = w_{\mathcal{O}}(5, 5) = (2.5, 2.5) \tag{53}$$
$$A^- = w_{\mathcal{O}}(1, 1) = (0.5, 0.5) \tag{54}$$
$$D_M^+ = \sqrt{(2.5 - 1.5)^2 + (2.5 - 1)^2} = 1.8 \tag{55}$$
$$D_M^- = \sqrt{(0.5 - 1.5)^2 + (0.5 - 1)^2} = 1.1 \tag{56}$$
$$b_M^T = \frac{D_M^-}{D_M^+ + D_M^-} = \frac{1.1}{1.8 + 1.1} = 0.38 \tag{57}$$

where $w_{\mathcal{O}}$ represents the weights assigned by the organization to each criterion for assessing adversarial interest (assume that it is transposed properly when multiplied against the adversarial interest scores), and A_M represents the weighted scores calculated based on the organization's scoring of adversarial interest in the Military Unit.

6.3 Combining asset criticality and adversarial interest scores

The combined score for the military unit, S_M^T, is then calculated by averaging the unit's asset criticality score, a_M, and its adversarial interest score, b_M^T. We also include S_M^{T51}, which emphasizes the unit-adjusted criticality score, and S_M^{T15}, which emphasizes the adversarial interest score.

$$S_M^T = \frac{a_M + b_M^T}{2} = \frac{0.54 + 0.38}{2} = 0.46 \tag{58}$$

$$S_M^{T51} = \frac{5 \cdot a_M + b_M^T}{5 + 1} = \frac{5 \cdot 0.54 + 0.38}{6} = 0.52 \tag{59}$$

$$S_M^{T15} = \frac{a_M + 5 \cdot b_M^T}{1 + 5} = \frac{0.54 + 5 \cdot 0.38}{6} = 0.41 \tag{60}$$

Table 13 shows the asset criticality scores, a_i, adversarial interest scores, b_i^T, and combined scores, S_i^T, S_i^{T51}, S_i^{T15}, for all units sorted by the combined score.

Table 13: *All calculated unit scores for unit-level example.*

Unit	a_i	b_i^T	S_i^T	S_i^{T51}	S_i^{T15}
HQ	0.47	0.38	0.43	0.46	0.40
Mil	0.54	0.38	0.46	0.52	0.41
CS	0.09	0.00	0.04	0.07	0.01
Res	0.06	0.83	0.45	0.19	0.70
IT	0.76	1.00	0.88	0.80	0.96

Table 14 shows how the different scoring methods affect the ranking of the units. Although the changes between ranking methods are not as dramatic as for the asset-level example, the rankings for this example appear to show that the simple average, S_i^T, gives the most intuitive ranking.

Table 14: *Unit ranking based on combined scores for unit-level example.*

Rank	**by** a_i	**by** b_i^T	**by** S_i^T	**by** S_i^{T51}	**by** S_i^{T15}
1	IT	IT	IT	IT	IT
2	Mil	Res	Mil	Mil	Res
3	HQ	HQ	Res	HQ	Mil
4	Res	Mil	HQ	Res	HQ
5	CS	CS	CS	CS	CS

7 Hybridization

In this section, we briefly look at how to combine the asset-level and unit-level methodologies to allow for more flexibility in implementation. By hybridizing the approaches, an organization need not commit to producing asset-level information for all its units in order to benefit from the asset-level methodology, nor must it discard unit-level results that might be of use to decision-makers. We discuss how to include unit-level information in asset-level results and asset-level information in unit-level results. We integrate a simple example throughout that is based on both the asset- and unit-level examples from Sections 4 and 6, respectively.

Table 15 shows the example data based on a combination of asset-level and unit-level information from previous examples. Two units, headquarters (HQ) and the military unit (Mil), provide asset-level information and, in addition, they categorize each asset into one of three unit-level asset categories: critical, essential, and non-essential. The remaining three units, corporate services (CS), research (Res), and information technology (IT) provide unit-level information.

7.1 Hybrid methodology for calculating asset-level results

We first look at how to integrate unit-level information into the asset-level level methodology presented in Section 3. The approach to calculating asset criticality is simple. For the units providing unit-level information, such as CS, Res, and IT in Table 15, we treat each asset category as a separate asset and follow the asset-level methodology for calculating asset criticality as normal. We ignore the weighting applied to the categories in the unit-level methodology because we assume that units will naturally rate critical assets higher than essential ones and essential assets higher than non-essential ones. We also ignore the number of assets in our calculation since it is unclear how this should affect the final ranking, if at all.

The approach to calculating adversarial interest for the unit's providing unit-level information is the same as the unit-level methodology. As we mentioned in the discussion of calculating adversarial interest for the unit-level methodology in Section 5.2, the asset categories do not necessarily have any relation to an adversary's interest in a unit's assets. What a unit might consider non-essential may be of significant strategic importance to our adversaries. Rather than try to redistribute or reclassify assets within asset categories based on adversarial interest, we apply the same overall unit-level adversarial interest scores to each asset category.

The results of this hybridized asset-level methodology are shown in Table 17. The ranking of the assets and asset categories based on these results is shown in Table 18. Again, the simple averaging of a_i and b_i^T given by S_i^T appears to give the most intuitive ranking.

Table 15: *Criticality criteria weights, asset category sizes and scores, and individual asset categories and scores for hybrid examples.*

	Number/ Category	**Importance**		
		of Asset	**of Data**	**to Others**
HQ weights		0.5	0.3	0.2
HQ.Comd	Essential	4	4	1
HQ.COSOps	Essential	4	4	1
HQ.AA	Non-essential	1	3	2
HQ.Files	Critical	4	5	5
Mil weights		0.4	0.4	0.2
Mil.CO	Critical	5	4	1
Mil.Adj	Essential	4	3	1
Mil.OpsO	Critical	5	4	1
Mil.SM	Essential	2	3	1
Mil.Files	Critical	5	4	4
CS weights		0.4	0.4	0.2
CS.Critical	0.1	2	5	5
CS.Essential	0.2	2	3	1
CS.Non-essential	0.7	1	1	1
Res weights		0.3	0.6	0.1
Res.Critical	0	1	1	1
Res.Essential	10	2	4	1
Res.Non-essential	30	2	1	1
IT weights		0.2	0.3	0.5
IT.Critical	20	5	5	4
IT.Essential	5	1	1	3
IT.Non-essential	2	2	2	1

Table 16: *Adversarial interest criteria weights, unit scores, and asset scores for hybrid examples.*

	Strategic importance	**Actor skill**
Weights ($w_{\mathcal{O}}$)	0.5	0.5
HQ.Comd	2	1
HQ.COSOps	2	1
HQ.AA	2	1
HQ.Files	3	2
Mil.CO	3	2
Mil.Adj	3	2
Mil.OpsO	3	2
Mil.SM	3	2
Mil.Files	3	2
HQ	3	2
Mil	3	2
CS	1	1
Res	5	4
IT	5	5

Table 17: *All calculated asset and asset category scores for asset-level results hybrid example.*

Asset	a_i	b_i^T	S_i^T	S_i^{T51}	S_i^{T15}
HQ.Comd	0.447	0.167	0.307	0.400	0.213
HQ.COSOps	0.447	0.167	0.307	0.400	0.213
HQ.AA	0.158	0.167	0.162	0.159	0.165
HQ.Files	0.564	0.383	0.474	0.534	0.413
Mil.CO	0.553	0.383	0.468	0.524	0.411
Mil.Adj	0.437	0.383	0.410	0.428	0.392
Mil.OpsO	0.553	0.383	0.468	0.524	0.411
Mil.SM	0.281	0.383	0.332	0.298	0.366
Mil.Files	0.659	0.383	0.521	0.613	0.429
CS.Critical	0.181	0.000	0.091	0.151	0.030
CS.Essential	0.105	0.000	0.053	0.088	0.018
CS.Non-essential	0.000	0.000	0.000	0.000	0.000
Res.Essential	0.123	0.833	0.478	0.241	0.715
Res.Non-essential	0.021	0.833	0.427	0.156	0.698
IT.Critical	0.806	1.000	0.903	0.839	0.968
IT.Essential	0.363	1.000	0.681	0.469	0.894
IT.Non-essential	0.137	1.000	0.568	0.281	0.856

Table 18: *Asset ranking for asset-level results hybrid example.*

Rank	**by** a_i	**by** S_i^T	**by** S_i^{T51}	**by** S_i^{T15}
1	IT.Critical	IT.Critical	IT.Critical	IT.Critical
2	Mil.Files	IT.Essential	Mil.Files	IT.Essential
3	HQ.Files	IT.Non-essential	HQ.Files	IT.Non-essential
4	Mil.CO	Mil.Files	Mil.CO	Res.Essential
5	Mil.OpsO	Res.Essential	Mil.OpsO	Res.Non-essential
6	HQ.Comd	HQ.Files	IT.Essential	Mil.Files
7	HQ.COSOps	Mil.CO	Mil.Adj	HQ.Files
8	Mil.Adj	Mil.OpsO	HQ.Comd	Mil.CO
9	IT.Essential	Res.Non-essential	HQ.COSOps	Mil.OpsO
10	Mil.SM	Mil.Adj	Mil.SM	Mil.Adj
11	CS.Critical	Mil.SM	IT.Non-essential	Mil.SM
12	HQ.AA	HQ.Comd	Res.Essential	HQ.Comd
13	IT.Non-essential	HQ.COSOps	HQ.AA	HQ.COSOps
14	Res.Essential	HQ.AA	Res.Non-essential	HQ.AA
15	CS.Essential	CS.Critical	CS.Critical	CS.Critical
16	Res.Non-essential	CS.Essential	CS-Essential	CS.Essential
17	CS.Non-essential	CS.Non-essential	CS.Non-essential	CS.Non-essential

7.2 Hybrid methodology for calculating unit-level results

We look next at how to integrate asset-level information into the unit-level methodology presented in Section 5. For the hybrid methodology calculation of asset criticality, the asset-level information needs to be supplemented with the assignment of an asset category to each asset as shown for the headquarters (HQ) and military units (Mil) in Table 19. The asset-level information can then be "rolled up" into unit-level asset categories by averaging the criteria for all assets in that asset category within the unit. The calculation of asset criticality can then be completed using the unit-level methodology. For the calculation of adversarial interest, the adversarial interest scores for the unit are simply the highest score for any unit asset in each criterion.

By design, the hybrid example scores given in Table 15 for headquarters (HQ) and the military unit (Mil) average to the unit-level example scores from Table 11. The sizes were increased for the unit-level example, but the ratio between categories was maintained. As a result, the data in Table 11 and Table 15 produce the same results and ranking for both the unit-level and hybrid methodologies. The results are reproduced here in Table 19 and Table 20, respectively, for ease of reading.

Table 19: *All calculated unit scores for unit-level results hybrid example. Same as Table 13.*

Unit	a_i	b_i^T	S_i^T	S_i^{T51}	S_i^{T15}
HQ	0.47	0.38	0.43	0.46	0.40
Mil	0.54	0.38	0.46	0.52	0.41
CS	0.09	0.00	0.04	0.07	0.01
Res	0.06	0.83	0.45	0.19	0.70
IT	0.76	1.00	0.88	0.80	0.96

Table 20: *Unit ranking based on combined scores for unit-level results hybrid example. Same as Table 14.*

Rank	**by** a_i	**by** b_i^T	**by** S_i^T	**by** S_i^{T51}	**by** S_i^{T15}
1	IT	IT	IT	IT	IT
2	Mil	Res	Mil	Mil	Res
3	HQ	HQ	Res	HQ	Mil
4	Res	Mil	HQ	Res	HQ
5	CS	CS	CS	CS	CS

8 Conclusion and future work

In this report, we proposed a way of introducing the concept of adversarial interest into how an organization measures the value, and especially the criticality, of its computer network assets. We presented a version of Kim and Kang's asset criticality approach from [1] that was modified to make it both meaningful and scalable for a large multi-unit, multi-mission organization. We showed how similar techniques can be used to score assets based on how likely they are to fulfil our adversaries' known strategic goals. We presented a number of methods for combining unit-adjusted asset criticality scores with adversarial interest scores to produce a list of assets ranked in their priority of importance to the organization. In addition to the asset-level methodology, we proposed a unit-level methodology that could be used where asset-level information may be hard to gather. Finally, we proposed a hybrid approach that would allow for units with asset-level information and units with unit-level information to combine their data to produce usable asset- or unit-level results.

Based on the asset-level, unit-level, and both hybrid examples in Sections 4, 6, and 7, respectively, we recommend the simple average, S^T, of unit-adjusted asset criticality and TOPSIS-calculated adversarial interest and the default combination method. We believe that, in the absence of further validation, this approach strikes a reasonable balance between prioritizing assets that are critical to our current operations and those that may be critical to our future operations.

As future work, we would seek to validate the best combination method. One approach to rigorously validating which method is best is to get feedback from experts in the field. We could get this feedback by holding a table-top exercise involving leaders and operators from the military cyber community. They would be asked both to rank the assets or units themselves and to use the proposed approach of scoring each of the assets or asset categories to produce rankings based on the various combination methods. They could then rate and comment on each of the resulting rankings, which will hopefully lead to a clear winner among the techniques. Nevertheless, care would need to be taken to ensure that the examples used during the exercise do not introduce biases in the exercise's results. Regardless of which technique is eventually chosen, we recommend the inclusion of a modifier in the final version so that the relationship between asset criticality and adversarial interest can be fine-tuned by the operators as needed.

One of the drawbacks of the asset-level approach proposed in this report is that it relies on organizations and units having intimate knowledge of how their computer network assets are used by their workforce and having the resources to maintain a usable record of that information. It is not always possible to know how computers get used. The computer in the corner that we discuss in the introduction may have been used months ago by the scientist researching gloves to download and discuss his research with one of the people in the military unit. Computer networks are designed to allow for the flexible use of assets in this way. A user from one part of the organization can log into a computer in another part by design. Unfortunately, this kind of flexible use is unlikely to be captured when the organization and units are asked to score their assets.

One way to get around the problem presented by the network's flexibility is not to rate the assets directly, but to rate the users. It is the users and their work that define the criticality of the computer network's assets. It is also the users and their work that is of strategic importance to our adversaries. Once we have rated the users, we can then score the assets based on who uses them. To this end, we have a contracted a forthcoming report that looks at how to tell which users are using which assets in a Windows 7 environment using native tools. The report specifically looks the importance of the asset based on who logs into it, the importance of the asset's data by who stores files on it, and the importance of the asset to others by who connects to the asset to use its service over the network. As future work, we would look at rating users and then using the information provided by the operating system or third party tools to automatically generate the criticality and adversarial interest criteria scores for each of the assets on the network.

List of acronyms/abbreviations

AFIT	U.S. Air Force Institute of Technology
AFRL	U.S. Air Force Research Laboratory
ARL	U.S. Army Research Laboratory
ARMOUR	Automated Computer Network Defence
CDMR	Cyber Decision Making and Response
CIMIA	Cyber Incident Mission Impact Assessment
CSDPAC	Cyber Security and Defence Preparedness Assessment Capability
DIMEI	Directorate Information Management Engineering and Integration
DRDC	Defence Research and Development Canada
DNS	Domain Name System
IT	information technology
MADM	multiple-attribute decision making
ORNL	Oak Ridge National Laboratory
SAW	simple additive weighting
TOPSIS	Technique for Order of Preference by Similarity to Ideal Solution

This page intentionally left blank.

References

[1] Kim, A. and Kang, M. H. (2011), Determining asset criticality for cyber defense, (Technical Report NRL/MR/5540–11-9350) Naval Research Laboratory.

[2] Beaudoin, L. (2006), Asset valuation technique for network management and security, In *ICDM Workshops 2006: Proceedings of the Sixth IEEE International Conference on Data Mining - Workshops*, pp. 718–721, IEEE.

[3] Grimaila, M. R., Mills, R. F., and Fortson, L. W. (2008), An automated information asset tracking methodology to enable timely cyber incident mission impact assessment, In *ICCRTS 2008: Proceedings of the 13th International Command and Control Research and Technology Symposia*, Office of the Secretary of Defense, U.S. Department of Defense, Command and Control Research Program.

[4] Goodall, J., D'Amico, A., and Kopylec, J. (2009), Camus: Automatically mapping cyber assets to missions and users, In *MILCOM 2009: Proceedings of the IEEE Military Communications Conference*, pp. 1–7, IEEE.

[5] Sawilla, R. (2006), Abstracting PageRank to dynamic asset valuation, (DRDC Ottawa TM 2006-243) Defence R&D Canada – Ottawa.

[6] Sawilla, R. and Ou, X. (2008), Identifying critical attack assets in dependency attack graphs, In *ESORICS 2008: Proceedings of the 13th European Symposium on Research in Computer Security*, Lecture Notes in Computer Science, pp. 18–34, Springer Berlin Heidelberg.

[7] Beaver, J. M., Patton, R. M., and Potok, T. E. (2011), An approach to the automated determination of host information value, In *CICS 2011: IEEE Symposium on Computational Intelligence in Cyber Security*, pp. 92–99, IEEE.

[8] Cam, H. (2012), PeerShield: Determining control and resilience criticality of collaborative cyber assets in networks, In *Cyber Sensing 2012*, Vol. 8408 of *SPIE Proceedings*, SPIE.

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Protected.)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

DRDC – Ottawa Research Centre
3701 Carling Avenue, Ottawa ON K1A 0Z4, Canada

2a. SECURITY MARKING (Overall security marking of the document, including supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Ranking assets based on criticality and adversarial interest

4. AUTHORS (Last name, followed by initials – ranks, titles, etc. not to be used.)

Kellett, M.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information. Include Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
August 2016	58	8

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Scientific Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Ottawa Research Centre
3701 Carling Avenue, Ottawa ON K1A 0Z4, Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
Project 05ac02	

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2016-R168	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11)) is possible, a wider announcement audience may be selected.)

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

We propose an approach to ranking computer network assets based on their criticality to an organization's current operations and business functions and their strategic importance to the organization's adversaries. An asset's criticality is a measure of its current importance to the organization, while an adversary's interest in the asset is a measure of its current importance to the adversary and, therefore, its future importance to the organization. We adapt techniques from existing work on asset criticality for use by a national defence organization. We also adapt these techniques to produce an adversarial interest score. We propose solutions for calculating these scores at the asset and the unit level and hybrid variants of both. We discuss options for combining asset criticality and adversarial interest scores to produce a list of assets or units ranked in order of their importance to the organization. The adversarial interest score can be used as an input to course-of-action recommendation algorithms. The combined ranked list of assets can be used by cyber defenders to prioritize the protection of assets within an organization.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus. e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

adversarial interest
asset valuation
asset criticality
adversarial interest
measures
metrics
technique for ordered preference by similarity to idea solution
TOPSIS

DRDC | RDDC

SCIENCE, TECHNOLOGY AND KNOWLEDGE FOR CANADA'S DEFENCE AND SECURITY | SCIENCE, TECHNOLOGIE ET SAVOIR POUR LA DÉFENSE ET LA SÉCURITÉ DU CANADA

www.drdc-rddc.gc.ca