

ABSTRACT FOR A PRESENTATION ON
Assessing the Contribution of Cyber-Attacks to Military Operations:
Applying the Value Creation / Value Destruction Model in a Non-Monetary Context
by Scott Borg
Director and Chief Economist
U.S. Cyber Consequences Unit

The method that the author originally developed to understand the cost of possible cyber-attacks to businesses and to the larger economy can be extended to apply to offensive military operations. This is possible for two reasons. One reason is that the model does not require the value-creating or value-destroying activities being assessed to be market-mediated, but can be applied to embedded systems. The other reason is the model does not require the value that is created or destroyed to be expressed in monetary terms, but can utilize other measures, such as lives lost or lives saved.

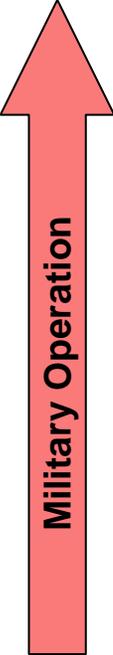
The key to the model is that it assesses all operations, whether business or military, in terms of inputs and outputs, and then compares the changes in inputs and outputs under different circumstances. It also considers the efficiency with which operational needs are matched with available resources.

A distinctive feature of the method is that it is profoundly holistic. It always starts with the outcomes of the total operation and then assesses the value contribution of the component parts. It never tries to add up the contributions of the component parts in an effort to deduce what value they would create when utilized together. This is vital, because in military operations, even more conspicuously than in business, the effect of the components working together can be vastly greater than their effect operating individually. (This is why equipment productivity models almost always yield the wrong answers.)

When this overall method is applied to certain operational scenarios, it leads to some startling conclusions. For at least a few likely scenarios, cyber-attacks do not appear to be a “force multiplier” or a means for increasing the return from a physical attack. They emerge as the “main event,” and the accompanying physical attacks appear to be a way of increasing the return from the cyber-attack.

The analysis could, in principle, be combined with certain methods from game theory in order to model what happens to both sides in a multi-round conflict where both sides are employing cyber-attacks in conjunction with physical attacks. But this more elaborate set of models is not necessary in order to apply the assessment to more limited military operations or to specific phases of larger campaigns.

The chart below summarizes the basics of this approach, although it probably requires considerable explanation in order to be interpreted correctly.

THE CONTRIBUTION OF CYBER-ATTACKS TO AN OFFENSIVE MILITARY OPERATION (BORG MODEL)		
 <p style="text-align: center;">↑ Gain in Damage to Target (Outputs)</p> <p style="text-align: center;">Military Operation</p> <p style="text-align: center;">Reduction in Resources Expended (Inputs) ↓</p>	<p>Increasing the Willingness-to-Pay</p> <ul style="list-style-type: none"> ● Increasing the yield from the attack <ul style="list-style-type: none"> ▪ increasing the permeability of defenses ▪ delaying the application of defensive measures ▪ increasing assurance of destruction (precision) ▪ increasing degree of destructiveness (lethality) ● Making the substitutes for the target less effective <ul style="list-style-type: none"> ▪ removing possible substitutes for the target ▪ delaying the switch to any substitutes 	<p>The Military Willingness-to-Pay Estimate:</p> <p>What it's worth to the attacker to force the defender to an alternative or fall-back operation (usually resulting in decreased losses for the attacker later or elsewhere)</p>
	<p>Decreasing the Opportunity Cost</p> <ul style="list-style-type: none"> ● Reducing the direct costs <ul style="list-style-type: none"> ▪ reducing the damage to the attacking force <ul style="list-style-type: none"> ▫ delaying the counter-attack ▫ reducing counter-attack yields ▪ reducing the time the attacking force will be needed ▪ reducing the supplies consumed by the attacking force ● Reducing the indirect costs <ul style="list-style-type: none"> ▪ reducing collateral damage to non-targets ▪ reducing public relations vulnerability 	<p>The Military Opportunity Cost Estimate:</p> <p>What the attacker is giving up by not deploying those resources in another way (which would force the defender to a fall-back operation in another context)</p>