A time-critical target (TCT) is one with a limited window of vulnerability or engagement opportunity during which it must be found, located, identified, targeted, and engaged. Perhaps the most familiar TCTs are mobile theater ballistic missile (TBM) launchers, which can “shoot and scoot.” In general, they can be detected while they are moving; in their “hides,” they are relatively invulnerable. Once the target is detected, a friendly weapon system must engage it before it returns to its hide.

The problem we are addressing in this chapter is that of an enemy submarine leaving port that is expected to submerge shortly. Like a stationary Scud launcher, a surfaced submarine is highly vulnerable. Submerging increases the difficulty of detecting, classifying, localizing, and killing it. For our example, we assume that the enemy submarine is detected as it leaves port and that an aircraft (or an Unmanned Combat Aerial Vehicle—UCAV—in the futuristic case) will use this cueing data (along with any subsequent updating data) as it tries to attack the submarine before it submerges.

We begin with a description of the vignette in the context of the general scenario presented in Chapter Two. Next, we present three alternative operating procedures and command and control structures designed to solve the problem. Finally, we apply measures and metrics of complexity and collaboration to each alternative and assess the impact each has on the ability to destroy the enemy submarine.
INITIATING EVENTS

On D+5 of the conflict, a U.S. Los Angeles-class SSN destroys an enemy attack submarine (SS) operating in the SLOCs northeast of the island. The enemy submarine commander was not able to report the attack to his headquarters on the mainland before sinking.

On D+6, a Virginia-class SSN begins a previously planned ISR mission off the enemy coast near the destroyed submarine’s home port.

Because the enemy is accustomed to irregular communications with its deployed submarines, it does not realize that its submarine has been killed until D+7. On D+8 a Kilo-class SS is ordered to replace the destroyed submarine. Kilo preparation begins the same day and “overhead” images indicate that the Kilo is preparing to go to sea. Its time of departure cannot be determined from the imagery. However, the Commander of the U.S. Joint Task Force (CJTF) is advised of the Kilo’s impending departure and, in turn, advises selected units.

A plan is devised to kill the Kilo on the surface as it emerges from the harbor without revealing the ISR submarine. An F/A-18 fighter-attack aircraft will be vectored to the Kilo and will kill it using a Standoff Land-Attack Missile–Extended Response (SLAM-ER) missile. The SLAM-ER will be guided to the area of the Kilo using a combination of the global positioning system (GPS) and an inertial navigation system (INS), and will acquire and kill it using an electro-optical passive seeker. The performance of this weapon depends on the accuracy with which target position is known at launch, with updates generated by the ISR submarine. An F/A-18 is prepared and placed in “Alert 5” status—it can be launched on five minutes’ notice. If necessary, the ISR SSN will step in and kill the Kilo even if this means compromising the ISR mission.

---

1The SLAM-ER is a high subsonic sea-skimming missile with the same electro-optical seeker as the AGM-64 Maverick (made famous in Operation Desert Storm). It uses the same cockpit display as the Maverick. It can work through object recognition or through laser designation. In operation, crosshairs are laid over the target the pilot is able to see. The SLAM-ER then guides itself to the designated target. If the target’s area of uncertainty (AOU) is excessive, the SLAM-ER electro-optical sensor may be unable to pick it up. In this case, the pilot can guide the SLAM-ER to reattack and try again.
The Kilo leaves port on D+10 under cover of darkness and is detected by the ISR submarine. Seeing the Kilo’s position, course, and speed on the surface, the ISR submarine estimates the remaining time until the Kilo submerges.

Figure 4.1 summarizes the initial events.

From this point, events are examined from the perspectives of 1980s platform-centric procedures, a current network-centric procedure, and a futuristic network-centric procedure using a UCAV in place of the F/A-18.

MEASURES OF PERFORMANCE AND EFFECTIVENESS

The paramount objective of the U.S. forces is to keep the enemy Kilo from reaching the SLOC north of the island. The JTFC has determined that this can best be accomplished by catching it on the surface and attacking it as early as possible. Nevertheless, the decision he must make is whether to dispatch an F/A-18 armed with a SLAM-ER to attack the Kilo or leave it to the Virginia-class SSN even though

NOTE: The circular fans along the enemy coast represent the extent of the enemy’s SAM coverage.

Figure 4.1—Initial Events
it is not considered to be the best platform to do this, given that its torpedoes are not optimized for shallow water. In addition, the attack by the SSN would give it away and compromise the ISR mission. The enemy will be unable to infer the source of targeting data relayed to attacking aircraft. The decision therefore hinges on the JTFC’s assessment of the time available to him to pursue the airborne option.

The command and control MOP selected for this analysis is Time on Target—i.e., the time available to an attacking aircraft to conduct its attack measured as the time elapsed between its arrival on station and the Kilo’s submerging. Since the actual time the submarine will submerge is not known to the CJTF, an earlier arrival time is better than a later one.

The combat MOE is the probability that the aircraft destroys the Kilo given that it arrives on station before the Kilo submerges. The operational impact on the ISR mission is measured in terms of hours of ISR mission lost to supporting an attack against the Kilo, given that the aircraft is unable to engage the target.

ALTERNATIVES

Three alternative operating procedures were developed to analyze this problem. Each makes assumptions about C4ISR systems, connectivity, and weapon systems. The first assumes little connectivity and platform-centric operations. The second assumes a richer network but with only slightly altered processes and equipment. The third assumes a richly connected network with new operating procedures and weapon systems. All three are defined below.

Platform-Centric Operations

Figure 4.2 depicts what is essentially a 1980s platform-centric approach to the submarine detection and acquisition problem. In this operational structure, the ISR SSN reports up the chain of command to the operational commander who then alerts the CVBGs that a threat submarine has left port (steps 2 and 3 in the figure). There is no direct communications between the F/A-18 and the ISR SSN. Note also that the operational commander does not control the ISR SSN, although periodic two-way communications is possible.
We assume that prior to the operation, the two carriers (one nuclear-powered carrier—CVN—and one conventionally powered carrier—CV) negotiate to determine which will provide the “ready” aircraft, that is, the aircraft that will be on strip alert ready for launch within five minutes (step 1 in the diagram). In this case, the CV is selected.

The CJTF develops the attack plan, using an F/A-18 armed appropriately and placed in “Alert 5” status on the CV (step 4 in the diagram). In this plan, an F/A-18 would fly out and attack the Kilo from outside the SAM envelope (see Figure 4.1) using a SLAM-ER missile (from a range of up to 150 nautical miles). The SLAM-ER will fly out to the estimated position of the Kilo.

The F/A-18 flies out to its launch point under operational control of the carrier, which may determine that the threat to the aircraft is excessive and abort the mission (step 5 in the diagram).

The ISR SSN will continue to provide updates on the Kilo’s position, course, and speed, but they will reach the F/A-18 through the opera-
tional commander as with the initial message and therefore the updates are likely to be considerably late (step 6 in the diagram). ²

Figure 4.3 summarizes the details of the SLAM-ER attack and possible reattack.

Command and control in this platform-centric case is split awkwardly between the SSN and air operations on the carrier. The SSN might see an indication that the Kilo was about to submerge and attack it without notifying the other units. In this case, the aircraft would continue on toward a launch point and might go on to an attack based on the last known Kilo position, course, and speed.

Air operations would vector the aircraft and feed it the latest update data. It could determine that the threat level to the aircraft was

---

²The diagram with shaded and white nodes at the left in Figure 4.2 is a network depiction of the connectivity. The shaded nodes represent entities directly involved in the operations, and the white nodes, although connected, represent facilities or combat entities that either monitor only or provide information. This same depiction is repeated in subsequent diagrams.
becoming excessive and, in that case, abort the mission. This would cause air operations to notify the operational commander that the aircraft mission was aborted and that data would be passed to the ISR submarine. The ISR submarine would ideally attack when the aircraft mission is aborted. Instead, in this vignette, it continues to pass target updates.

**NETWORK-CENTRIC OPERATIONS**

In this second case, the connectivity among the participants is richer, as depicted in Figure 4.4. The Virginia-class ISR submarine has two-way communications (via Link 16) to the carriers. As in the platform-centric case, the ISR submarine also has two-way communications to its operational commander, but these communications can be regarded as “courtesy copies.” The fact that the ISR submarine has direct communications to the controlling carrier (and the deploying aircraft) obviates the need to rely on the operational commander to relay messages. Nevertheless, the operational commander monitors communications with the SSN.

![Figure 4.4—Network-Centric Operations](image-url)
The controlling carrier uses two-way communications with the F/A-18 to control its operation and to confirm threat status updates. The F/A-18 receives periodic target updates directly from the ISR submarine with latency stemming mainly from security considerations (steps 4 and 5 in the figure).

As in Figure 4.3, the F/A-18 will fly outside the SAM coverage envelope to the SLAM-ER launch point and then guide the missile to Kilo acquisition. Relative to the platform-centric process, the area of uncertainty has been reduced to just over one square nautical mile.

The command and control architecture for this version of network-centric operations has the same divisions as the previous platform-centric operation architecture but the consequences of this division are considerably reduced. For example, the ISR submarine may still decide on its own that the Kilo is about to submerge and that the aircraft cannot attack in time and so attack the Kilo itself. However, with communications directly to the carrier, the aircraft can be turned back earlier.

Similarly, if air operations determines that the threat level to the F/A-18 is excessive, the aircraft can be turned back unilaterally. The ISR submarine can be alerted to the situation in its next communication cycle, and therefore it will have more time to attack the Kilo itself.

Future Network-Centric Operations

The Navy’s UCAV concept is currently under consideration by the Office of Naval Research (ONR).\(^3\) UCAVs are designed to be launched from a variety of surface combatants in theater and would therefore be an attractive option in this scenario, in that it would relieve the Navy’s burden of keeping an F/A-18 (and a catapult) on

---

\(^3\)The UCAV is designed to be a highly maneuverable, autonomous, Vertical and/or Short Takeoff and Landing (V/STOL) aircraft capable of operating from air-capable ships (other than carriers). It will provide multimission capability including surveillance, target recognition, and air combat to the mother ship. This will involve the development of intelligent control for vision-based navigation, guidance and control, self-optimizing, learning control schemes accepting input from multiple sensory agents and from hierarchies of decisionmaking, and intelligent augmentation for human-centered decisionmaking. See http://robotics.eecs.berkeley.edu/~sastry/onr/ucav/prop/node2.html for more information.
Alert 5 status for days. For the purpose of NCW analysis, we assume that a UCAV will be developed and deployed by the 2010 time frame.\(^4\)

Figure 4.5 depicts the operating environment with UCAVs deployed on a destroyer and a cruiser in the theater of operations.\(^5\) Note the increase in connectivity among the participants in this case from the notional diagram in the lower left of the figure and the geographical depiction.

After the ISR submarine detects the Kilo coming out of port it alerts all potential UCAV launch ships within the limits of its security

---

\(^4\)At the time this research was conducted, Navy plans were as stated in the text. However, the Navy with Defense Advanced Research Projects Agency (DARPA) support has since moved toward a UCAV platform of aircraft proportions that could only operate from aircraft carriers.

\(^5\)In principle, several other surface combatants might carry the UCAVs. However, for simplicity, we focus on the two platforms only.
concerns (step 1). The ships receiving the message negotiate to determine which can get a UCAV to the Kilo first (step 2). The time to launch a UCAV and UCAV fly-out times would be the determining factors.

In arriving at a decision, the combatants with UCAVs collaborate with each other and with other facilities with information needed to arrive at a best solution. Such issues as who makes the final selection, who determines when sufficient collaboration has occurred, what prior designations have been made, what is the polling frequency, and who determines which combatants with UCAVs are candidates are command and control procedural questions that must be addressed and evaluated analytically.

A UCAV is then launched and begins its fly-out to the Kilo area of uncertainty (AOU) (step 3).

The ISR submarine takes over control of the UCAV, including weapon release (step 4). If the ISR submarine realizes that it must attack the Kilo due to the UCAV's late arrival, the UCAV will be turned back at the next communications cycle. If the submarine determines that the risk of losing the UCAV is becoming excessive (i.e., that UCAV probably will not survive to the launch point), it can conduct the attack and turn back the UCAV itself much more quickly.

The command and control architecture for this case is unsettled. Several options are available, and three of these are listed in Table 4.1. The impact of each option listed in the table is somewhat speculative. However, these (and other possibilities) constitute the basis for conducting exploratory analysis to determine the effects of each on combat outcomes. The results of the analysis of these three options and several variants are reported in Chapter Five.

In addition to the options listed in Table 4.1 are those associated with decentralized command and control. For example, it is possible to establish objective response criteria a priori and apply them at execution time. With all ships sharing the same COP, each can determine the ship most suitable to respond without the intervention of a centralized authority in some form of a bidding process. True decentralized execution then is based on negative control procedures, i.e.,
A Time-Critical Target 77

Table 4.1
Future NCW Command and Control Variants

<table>
<thead>
<tr>
<th>Option</th>
<th>Process</th>
<th>Impact on Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete polling</td>
<td>Poll all potential combatants with UCAVs and select the one that can</td>
<td>Large cost in collaboration time</td>
</tr>
<tr>
<td>at execution time</td>
<td>get to the target quickest</td>
<td></td>
</tr>
<tr>
<td>Periodic selection of</td>
<td>Poll a select subset of combatants with UCAVs considered to be in the</td>
<td>Fastest fly-out time for UCAV after decision is taken</td>
</tr>
<tr>
<td>a subset of combatants</td>
<td>best position to respond. Repeat this process periodically</td>
<td></td>
</tr>
<tr>
<td>with UCAVs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Periodic complete</td>
<td>Poll all combatants with UCAVs periodically and designate one as the</td>
<td>Moderate cost in collaboration time</td>
</tr>
<tr>
<td>polling of combatants</td>
<td>“duty” launcher</td>
<td>Possibly greatest fly-out time for the UCAV after decision is taken</td>
</tr>
<tr>
<td>with UCAVs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: In this context, “polling” is a request from a central authority for information essential to selecting one of the candidate ships with UCAVs to execute the TCT mission. Polling may or may not be automated.

the ship deemed most suitable executes unless vetoed by the JTFC. These procedures are also candidates for further analysis using the measures and metrics proposed below.

LATENCIES

For each of the three cases studied, the time required to perform the required tasks is central to computing the latency MOP necessary to evaluate the effectiveness of TCT operations. Table 4.2 lists the expected (mean) times required to complete the tasks listed along with a reasonable upper bound (the lower bound is, of course, 0). All times are stated in minutes and are converted to hours in the spreadsheet model presented in Chapter Five.
# Table 4.2

## Expected and Maximum Latencies

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Platform-Centric</td>
</tr>
<tr>
<td></td>
<td>Mean</td>
</tr>
<tr>
<td>ISR SSN alert</td>
<td>15</td>
</tr>
<tr>
<td>SubGroup processing</td>
<td>20</td>
</tr>
<tr>
<td>CV reads, processes, alerts flight operations</td>
<td>10</td>
</tr>
<tr>
<td>CV directs aircraft</td>
<td>2</td>
</tr>
<tr>
<td>Select launch platform</td>
<td>—</td>
</tr>
<tr>
<td>Aircraft preparation and launch</td>
<td>5</td>
</tr>
<tr>
<td>UCAV launch</td>
<td>—</td>
</tr>
<tr>
<td>UCAV fly-out</td>
<td>—</td>
</tr>
<tr>
<td>F/A-18 fly-out</td>
<td>15</td>
</tr>
<tr>
<td>SLAM-ER fly-out</td>
<td>15</td>
</tr>
<tr>
<td>SSN update</td>
<td>15</td>
</tr>
</tbody>
</table>

**NOTE:** All times are in minutes.

## Platform-Centric Latencies

Communications latencies begin with an alert that the Kilo has left port. Security concerns prevent the ISR SSN from communicating this data immediately. The expected alert latency is estimated to be 15 minutes for the purpose of this study and 60 minutes at most. Note that latencies apply only to the initial alert notice. The ISR SSN will be unable to update the Kilo’s position, course, and speed continuously (giving one update on average every 15 minutes and at worst every hour). Data will be current at time of transmission.

Using procedures in effect in the 1980s, the mean time for a submarine group to receive, digest, and retransmit the information from the ISR SSN is 20 minutes with a maximum time of 45 minutes.

---

6These time estimates, and all others in this vignette, are based on discussions with the former commanding officer of an SSN that conducted a similar ISR mission.
At the carrier, the information from the submarine group is read at
the Carrier Intelligence Center (CVIC) and extracted to reduce classi-
fication level. The information is then conveyed to air operations.
The mean time for this manual process is estimated to be 10 minutes
with a maximum of 20 minutes.

The update information is then communicated to the F/A-18 with a
short delay (estimated at two minutes on average with a maximum of
five minutes).

Total latency in alerting the carriers is estimated to be 35 minutes on
average with a maximum of 105 minutes. Updates to the aircraft are
estimated to be just over half an hour on average (32 minutes) with a
maximum of 70 minutes. This means that, on average, the F/A-18
will have half-hour-old targeting data at the time of attack. The tar-
get area of uncertainty is about 20 square nautical miles for this type
of operation.

In terms of operational delays, there will be a delay from the time air
operations receives the alert to F/A-18 launch time. This is taken to
be five minutes on average and 10 minutes at most (the F/A-18 was
kept in Alert 5 status). It must fly out (taken to be 15 minutes on av-
erage and 30 minutes at most) to its launch point, with expected
SLAM-ER fly-out estimated also at 15 minutes with a maximum time
of 20 minutes. It must be launched outside the SAM envelope but
within 150 nautical miles of the target.

Several of these latencies will apply in the next two cases as well and
therefore they will not be repeated.

**Network-Centric Latencies**

The time lapse from detecting Kilo egress from port to the alert no-
tice is unchanged. It is still driven by the ISR submarine’s security
concerns. However, the alert notice and subsequent updates are
now delivered directly to the CVIC. Those updates will then be con-
veyed to air operations within the carrier.

In terms of operational delays, there is no difference from the previ-
ous case. It will still take five minutes to launch the Alert 5 aircraft on
average, and so on.
Future Network-Centric Latencies

In this case, using the UCAV, the alert messages go out to the submarine group and to the carriers as before. However, a request for a UCAV is sent at the same time to surface combatants with UCAVs in the area of operations. The UCAV ships negotiate to determine which can get a UCAV to the Kilo first, and that ship launches a UCAV. Control of the UCAV is transferred to the ISR submarine.

The distinctive feature of this case is that, whereas an Alert 5 aircraft can be readied days in advance, the decision to designate a surface ship to launch the UCAV is conducted in real time. This is because, as ships move about and ship status changes, the best ship for launching a UCAV can change dynamically.

In this vignette, it is apparent that a UCAV can reach a weapon launch point before an F/A-18 could—it has a significantly shorter flight distance. This is represented by an average five-minute and maximum 10-minute fly-out time for the UCAV as opposed to an average of 15 minutes and a maximum of 30 minutes of fly-out time for the F/A-18. Offsetting this potential advantage is the additional delay imposed while the UCAV ships negotiate to determine the best launch platform (not represented explicitly in Figure 4.5). It is conceivable that, with enough ships in the network, flight time reduction would be more than offset by the additional time required to select a launch platform.

A PROBABILITY MODEL OF KNOWLEDGE

The uncertainties in the TCT problem center on the time required to get ordnance on target. The intermediate times used to collect, process, and disseminate information, all of which are also uncertain, contribute to this time. Because they are uncertain, all are considered to be random variables. They all have the same characteristics in that the likelihood that the task will be completed increases with time. This behavior can best be described with a Gamma distribution, $\Gamma(\alpha, \lambda)$. For this work, we chose the exponential distribution, the special case of the Gamma where $\alpha = 1$. This is made more explicit later. For now, we consider the time, $t$, required to complete one of the tasks in the TCT problem, where $t$ is a random variable with density function:
The expected (mean) time required to complete the task is $1/\lambda$ minutes. The uncertainty in this and the other times constituting the overall TCT problem can be taken to reflect a lack of knowledge. Knowing exactly how long each task takes facilitates planning and execution—a lack of knowledge can result in poor planning and mission failure. Consequently, it is important to quantitatively assess the knowledge possessed by the decisionmaker at the time a decision must be taken. As in the missile defense vignette discussed in Chapter Three, we turn to the field of information theory and the concept of information entropy or the average information in a probability distribution to characterize knowledge.

**Information Entropy**

Recall from Chapter Three that information entropy (or Shannon entropy) is a measure of the average amount of information in a probability distribution and is defined as:

$$H(t) = -\int_{t=0}^{\infty} \ln[f(t)]f(t)dt.$$ 

Applying this to the exponential distribution we get:

$$H(t) = \ln\left(\frac{e}{\lambda}\right).$$

This suggests the following definition for the knowledge associated with the latency distribution:

$$K(t) = \begin{cases} 0 & \text{if } \lambda < \lambda_{\min} \\ \ln(\lambda/\lambda_{\min}) & \text{if } \lambda_{\min} \leq \lambda < e\lambda_{\min} \\ 1 & \text{if } \lambda \geq e\lambda_{\min} \end{cases}$$

---

7 The inverse, $\lambda$, is therefore the number of these tasks that can be accomplished in a unit time (minute).

8 A complete derivation of this term can be found in Chapter Three.
One problem with this formulation is the condition for “perfect” knowledge. This occurs when $K(t) = 1$ or when the expected time to complete a task, $1/\lambda$, is approximately one-third the maximum expected time to complete the task. It may be desirable in some cases to employ more stringent conditions on “perfect” knowledge. This can be accomplished by casting the probability distribution in terms of $M > e$. Although the distribution would not be exactly the form of the exponential with $e$ as the base, it will have a similar form and the condition for “perfect” knowledge will be more stringent. Figure 4.6 illustrates the knowledge function for $\lambda_{\text{min}} = 0.5$ completions per hour, or a maximum time of two hours to complete a task.

**MOP**

We start by assessing the performance of the command and control system in both a platform-centric and network-centric environment.

![Figure 4.6—The Knowledge Function](image-url)
The MOP is *time-on-target*. This is defined as the time elapsed from the moment the target becomes vulnerable or can be engaged to the time it is no longer vulnerable or cannot be engaged. In our example, this is the time available for the aircraft (or UCAV) to fly out to the AOU, and detect, target, and kill the enemy submarine before it submerges. Minimizing this accumulated time increases the likelihood that the mission can be accomplished before the submarine submerges and is therefore an appropriate measure of system performance.

Instead of treating the time the Kilo submerges as a random variable and thus introduce additional uncertainty, we instead treat it parametrically. In addition, we assume that no uncertainty exists about the location of the target in that the *Virginia*-class SSN is tracking the Kilo.

Determining time-on-target seems rather simple—i.e., just subtract the latency from onset of target vulnerability to time of engagement from the total time of vulnerability. However, subtleties must be considered.

**The Operational Network as a Graph**

We begin by describing the command, control, and communications network supporting the operation as an abstraction of a directed graph. A graph, \( G(X, E) \), is composed of a set of nodes, \( X = \{x_1, x_2, \ldots, x_n\} \), and a collection of edges, \( E = \{e_1, e_2, \ldots, e_m\} \), joining all or some of the nodes. Suppose we have a notional network that consists of \( n \) nodes with \( m \) edges. Framing the discussion in terms of a command and control system, we refer to the edges as *connections* and we refer to the graph as the *network*. By “connection,” we mean that the “connected” nodes are able to communicate to each other directly. This does not necessarily mean that there is a physical connection between the two. Each connection may have a component that indicates the direction in which the communication of information may flow between nodes. Connections where the communications flow is unidirectional are called *directed connections*. In Figure 4.7, the communication between nodes 6 and 8 is two-way, but the flow of information between nodes 8 and 9 is directional (node 8 may pass information to node 9 but may not receive information directly from node 9). If at least one connection in the network \( G(X, E) \) is
directed, we refer to the network as a *directed network*. If no connection is directional, the network is *nondirected*. When a network is directed, we refer to the transmitting node as the *initial node* and the receiving node as the *terminal node*.

Of the *n* nodes in the network, however, only *τ* are involved in the current operation. The shaded nodes represent those involved in the operation. This is typically the structure of operational networks. Not all potential operational elements are connected and not all are involved in the current operation. For example, Figure 4.7 illustrates a network with 10 nodes but only three are participating in the current operation. There are 15 connections (11 with a single com-
communications direction and two that are bi-directional: $11 + (2 \times 2) = 15$ in the total network but only three connections (one one-way and one two-way $= 1 + (1 \times 2) = 3$) between nodes participating in the current operation.

Some interesting relationships arise from this topology however. First, we note that the maximum number of connections in an undirected network with $n$ nodes is:

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

In this case, we have that $m \leq \lfloor n(n-1) \rfloor / 2$. In a directed network with $n$ nodes, the maximum number of connections is $n(n-1)$ so that $m \leq n(n-1)$. If all the nodes in a graph are connected, the graph is referred to as being complete. In the directed network in Figure 4.7, we have a maximum 90 possible connections.

Second, it is important to analyze the role of connected facilities not directly involved in the operation. For example, nodes 6 and 8 are connected to node 7. If node 7 were the CJTF controlling the operation, then 6 and 8 might be information sources (fusion centers on board or remotely located, national intelligence centers, etc.) available to the CJTF. These connections allow the participants to collaborate in arriving at a decision. We expect that collaboration in this case improves the quality (accuracy, timeliness, and completeness) of the decision and is therefore an attribute of the command, control, and communications process that needs to be factored into the overall metric.

**The $n^2$ Phenomena**

More important than counting the number of connections of one type or another is the value of the connections — i.e., their contribution to combat outcome. If we examine the complete directed graph, we see that there are $n(n-1) = n^2 - n$ connections. If we assume that all connections contribute to the value of the network, then more connections are desirable. Logically, we conclude that for a very large $n$, the first term, $n^2$, dominates and therefore the value of the network increases as the square of the number of nodes in the
network increases. This is referred to as *Metcalf's Law*, named for Robert Metcalf, a pioneer in the development of the Ethernet.\(^9\)

The problem with this assessment of a network’s value is that it assumes that all interactions are equally “valuable”—that is, that they all contribute an equal positive amount to the value of the network. This is clearly not always the case. The problem of assessing the true value of the network in terms of its contribution to combat outcomes is much more complex.

**Too Much Information**

Another “law” governing connected networks deals with the propensity of people to utilize available connections to transmit information that may or may not be useful to the recipient. Simply stated, the larger the number of connections in an operational network, the more likely individual nodes will experience “information overload.” This is simply a paraphrased Parkinson’s Law that “work expands to fill the time available.” That is, if a communication channel exists it is likely to be used. This too is compelling—however, like Metcalf’s Law it does not apply universally. With proper filtering, extraneous communications can be controlled, especially during critical operations.\(^10\) However, anecdotal evidence seems to confirm that instances of “information overload” occur over undisciplined networks.

**Latency**

Although not the complete story, the time required to get a weapon on target is an important part of the time-on-target metric. In general, \(\tau \leq n\) nodes are involved in the operation. We will refer to these

\(^9\)Robert Metcalf is credited with discovering the Ethernet. He was also founder of the 3Com Corporation of Santa Clara, California, in 1981, the leading producer of Ethernet adapter cards. An interesting discussion of Metcalf and his “law of the telecosm” can be found in Gilder (1993). See also Appendix A to Alberts, Gartska, and Stein (1999).

\(^10\)The actual quote is: “Data expands to fill the space available for storage.” Buying more memory encourages the use of more memory-intensive techniques. Those of us who use computers have experienced the wisdom of these words. See, for example, Parkinson (1957).
nodes as the \textit{task force}.\textsuperscript{11} Not all need be combat elements; some may be sensors, information processing facilities, etc. The only criterion is that they be directly involved in the mission. The time required for each to perform its assigned tasks contributes directly to latency. Note that we are not concerned about "how well" they perform their task at this point—just how long it takes. It is also possible that the elements of the task force perform their tasks in parallel, sequentially, or some combination of both.

For node $i$, the time, $t$, required to perform all of its tasks in support of the operation is taken to be a random variable with exponential distribution:

$$f(t) = \lambda_i e^{-\lambda_i t},$$

where $1/\lambda_i$ is the mean time to complete all tasks at node $i$. Assuming that all nodes act sequentially, we then get a total expected latency of

$$L = \sum_{i=1}^{\tau} \frac{1}{\lambda_i}.$$

Other operating concepts are possible. For example, Figure 4.8 depicts two different concepts, both of which have sequential and parallel processing components. The expected latency for the first concept is:

$$L_1 = \max \left\{ \left( \frac{1}{\lambda_6} + \frac{1}{\lambda_7} + \frac{1}{\lambda_8} \right) \left( \frac{1}{\lambda_6} + \frac{1}{\lambda_9} + \frac{1}{\lambda_8} \right) \left( \frac{1}{\lambda_6} + \frac{1}{\lambda_5} + \frac{1}{\lambda_8} \right) \right\},$$

$$L_2 = \max \left\{ \left( \frac{1}{\lambda_6} + \frac{1}{\lambda_7} + \frac{1}{\lambda_8} + \frac{1}{\lambda_9} \right) \left( \frac{1}{\lambda_6} + \frac{1}{\lambda_5} + \frac{1}{\lambda_9} \right) \right\}.$$

\textsuperscript{11}In graph-theoretic terms, this is called a subgraph, $G_s(X,E)$, that contains only a subset of the nodes in $X$, but contains all of the edges whose initial and terminal nodes are within the subset. Applied to command and control, a subgraph is a subnetwork.
Figure 4.8—Alternative Operating Concepts

Note that only the path nodes are assessed, not the transit time between the nodes. The reason is that we are assessing the delay at the nodes only: The communication time between nodes is taken to be practically instantaneous.

In either case, the critical path times constitute the expected latency. If we let $\rho \leq \tau$ represent the number of nodes on the critical path, the expected latency then is:
\[ L = \sum_{i=1}^{\tau} \delta_{ii}, \]

where

\[ \delta_{ii} = \begin{cases} 1 & \text{if node } i \text{ is on the critical path} \\ 0 & \text{otherwise} \end{cases}, \quad \text{and} \quad \sum_{i=1}^{\tau} \delta_{ii} = \rho. \]

Also observe that if the effective times required for critical path nodes to complete their tasks are sufficiently reduced, a new critical path may emerge.

**Information Quality**

In our example, the quality of the information about the location of the enemy submarine is influenced in several ways by the command, control, and communications system. First, the equipment and procedures in place at each of the nodes that contribute to the operation affect the accuracy of the intermediate products produced at that node. For example, the fusion facilities on board the cuing system determine, in part, how well the enemy submarine is tracked. Second, the degree to which the task force is able to collaborate to inform decisions and ensure that a complete picture is at hand increases the confidence that a correct (accurate) decision will be taken. Third, the ability of the task force to access other nodes in the network to complete the operational picture helps ensure nothing is missed. Finally, the amount of training and level of experience of the crews and the length of time they have operated as a team affect the speed with which they are able to accomplish their assigned task—to locate and engage the enemy submarine.

A comprehensive measure of quality therefore would include elements of accuracy, completeness, and timeliness. A validation and calibration process would include adequate representations of each. However, for this work, a suitable measure of quality was taken to be the amount of knowledge available about the expected times required to complete tasks. The quality of the processes and equipment in place at each node, \( i \), in the task force is calculated as the knowledge function, and therefore we have a metric, \( 0 \leq K_i(t) \leq 1 \).
value of $K_j(t)$ close to 1.0 implies high quality, whereas one nearer to 0 implies low quality. In addition to the nodes in the task force, we assume that the quality of the products produced by other nodes in the network can also be measured in the same way.

**Collaboration’s Effect**

In Chapter Three, collaboration was defined as a process in which a team of individuals works together to achieve a common goal. It was argued that collaboration enhances the degree of shared awareness in a group focused on solving a specific problem or arriving at an agreed-on decision. In the TCT problem, collaboration consists of sharing information, among the task force members and others in the network, needed to accomplish the mission of locating and engaging the enemy submarine. In general, therefore, collaboration can contribute to the network’s ability to support combat operations.

Before we assess the contribution of collaboration to the task of locating and engaging the enemy submarine, we need to expand our discussion of graph theory to include the definition of the *indegree* of a node:

**Indegree:** The indegree of a node, $x_i$, in a directed graph is the number of edges that have $x_i$ as their terminal node.\(^{12}\)

The network graphs in Figures 4.7 and 4.8 are directed graphs. Note that node 6 in Figure 4.7, for example, has indegree 4.

The opportunity for collaboration depends on the number of task force and other nodes each task force node is connected to, or the indegree of the node.

The quality of collaboration as represented by the collective knowledge of the collaboration team has the *effect* of reducing the amount of time required to complete the task (take a decision, order its execution, and take the action required). This is an important point because it may be the source of confusion here and later in the text. By “effectively” reducing the time required, we recognize that although quality collaboration may in fact have no effect on the “actual” time

---

\(^{12}\)Taken from Christofides (1975). See also Jackson and Thoro (1990).
required to complete the task, it does provide the opportunity to use the time available more wisely and therefore makes an improvement in the quality of the eventual outcome of the operation more likely. An advantage of this approach is that it can be used to express the quality of collaboration in terms meaningful to operators by translating it into additional time to perform a task or mission.

We should also add here that clearly other factors could be taken into account besides the amount of time required to complete tasks. Each node may contribute something unique to the process, and its ability to do so may be uncertain. This gives rise to the possibility that several random variables, some dependent and others independent, are in play at each node. Combining these uncertainties to form a comprehensive knowledge function is the subject of future research.

For a directed connection, if the quality of the interaction between the terminal task force node, \( i \), and any other connected initial node, \( j \), is “good,” then \( K_j(t) \) will be close to 1. This represents the fact that node \( j \) is able to supply quality information to the executing node. If \( K_j(t) \) is large, then \( 1 - K_j(t) \leq 1 \) will be small and when multiplied with the actual mean time to complete the task, \( 1/\lambda_i \), will produce an effective latency smaller than the actual latency, \( 1/\lambda_i \).

If we let \( d_i \) be the indegree of the task force node \( i \), then the contribution of quality collaboration to node \( i \)'s operation can be expressed as the product:

\[
c_i(t) = \prod_{j=1}^{d_i} (1 - K_j(t))^{\omega_j}
\]

where

\[
\omega_j = \begin{cases} 
0.5 & \text{if node } j \text{ is not in the task force} \\
1.0 & \text{if node } j \text{ is in the task force}
\end{cases}
\]

The exponent, \( \omega_j \), accounts for the relative importance of the collaboration between two nodes. In this case, in the absence of any experimental data, we use only two levels: important (0.5) and very important (1.0). Perhaps a richer distribution would more accurately
reflect the nuances in the effectiveness of the collaboration and its effect on latency, but that remains for further analysis through experimentation.

The total effective latency accounting for collaboration is therefore:

\[ L_c = \sum_{i=1}^{\tau} c_i = \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} \left(1 - K_j(t)\right)^{10_j} \delta_{L_i}. \]

The effect of collaboration is to reduce the total expected time required to complete the mission, and “good” collaboration reduces it further.\(^\text{13}\)

**Complexity**

The concept of network complexity was introduced in Chapter Three, where we deferred the detailed discussion of the subject to this chapter, where its application is easier to assess.

Acting counter to Metcalf’s Law, we have noted that in a well-connected network (however large) the possibility always exists that too much information is made available to the task force nodes, resulting in what is generally referred to as “information overload.” This can have the opposite effect of collaboration. Instead of effectively cutting the time required to complete tasks, it can prolong the time as staff and commanders sift through the information for what is required. On the other hand, a richly connected network with a well-disciplined command and control system installed can facilitate decentralized decisionmaking and execution and therefore improve the effectiveness of combat operations as well as reduce the time needed to process information.

Network complexity therefore can have both good and bad effects. In this work, we assess the benefits of complexity in terms of collaboration effects and the negative effects of information overload as a factor that increases the time required to perform necessary tasks. It

\(^\text{13}\)Note that if one of the quality metric values for a node collaborating with a task force node is 1.0, the time required for the task force node to complete its task is 0. However, the method of calculating the quality metric prevents this from happening.
should be noted, however, that we can mute the negative effects by suitable selection of parameters in the complexity metric.

Complexity then is a function of the total number of connections to the task force nodes, or the total indegree of the operation. Therefore, complexity focuses on the potential misuse of the network, whereas collaboration focuses on the effective use of the network. If we let $C$ represent the total number of connections in the network, then

$$C = \sum_{i=1}^{\tau} \delta_i \nu_i.$$  

For small values of $C$, the complexity effect is negligible, and for some range it increases rapidly, leveling off at what might be referred to as the information overload point—i.e., when the information arriving from the multiple connections is so great as to practically shut down operations. Although the exact functional relation is not known, a logistic or S-curve relation between $C$ and the complexity factor exhibits the appropriate behavior. If we let $g(C)$ represent the complexity factor, we have:

$$g(C) = \frac{e^{a+bC}}{1+e^{a+bC}}.$$  

The parameters $a$ and $b$ determine both the region of minimal impact and the size of the region of rapidly increasing impact. Figure 4.9 illustrates a typical complexity function for the 0 to 90 possible connections for the network depicted in Figure 4.7. Including complexity in the calculation of expected latency, we get:

$$L_{CC} = \frac{1}{\lambda^{a+bC}} \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} \left[ (1-K_j(t))^{\nu_j} \right] \delta_i.$$  

---

14The actual relationship should be established through experimentation.

15Assuming the logistic curve is the appropriate model for the complexity factor, selecting the coefficients is problematic. They are clearly application-specific and therefore best derived from experimentation. Those depicted in this report are notional.
When the number of connections is low, the complexity effect on latency is minimal. Between about 30 and 60 connections, the complexity effect rises sharply, leveling off to near paralysis at 90.

**Effective Expected Latency**

Equation (1) reflects the balance between the positive effects of collaboration and the negative effects of complexity. If the effects of complexity are negligible—i.e., there are few connections in the network—and the effects of collaboration are considerable—i.e., the knowledge function for most distributions is high—then it is possible for the expected latency to be much lower than the sum of the critical path latencies. This means that the positive effects of collaboration have compensated for the time required to perform all operational tasks. The converse is also true in a richly connected network where
the knowledge functions are rather small. That is, the effective latency can exceed the critical path latency. For this reason, we refer to $L_{cc}$ as the “effective expected latency.”

MOE

The measure of TCT effectiveness used here is simply the probability that the target can be attacked during the window of opportunity. For the case of the surfaced threat submarine, it is the probability that the aircraft can detect, classify, and place ordnance on the submarine before it submerges. This probability of detection depends on time on target, the quality (accuracy, timeliness, and frequency) of the location and speed estimates of the enemy submarine, and the characteristics of the attack weapon. For the purpose of illustration, we assume that the aircraft will attack using a missile with an electro-optical system that can detect and classify the threat submarine on the surface. The aircraft is not expected to detect the submarine directly. The pilot will use the cockpit display from the missile to detect and classify the target. The pilot will then lock the missile onto the target. For simplicity, we regard the aircraft as searching the AOU about the target submarine, with the missile used as a remote sensor. We assume a sea-skimming missile with an accordingly short acquisition range, and that once the missile has acquired the submarine it will be killed quickly. In other words, we ignore time of flight over the acquisition range and weapon reliability.

Detection and Target Acquisition

If $S$ is the time elapsed between the moment the submarine leaves port and submerges (in hours), then $T = S - L_{cc}$, where $T$ is the effective search time. If $T \leq 0$, the aircraft fails to engage the target. If $T > 0$, the cumulative probability that the aircraft detects and acquires the target depends on the time it must search the AOU.\(^\text{16}\)

If we let $q(T) = 1 - P_d(T)$, where $P_d(T)$ is the probability of detection as a function of search time, then $q(T)$ is the probability that there

\(^{16}\)For purposes of this analysis, we are concerned with both detection and acquisition. However, for ease of exposition in the sequel, we refer to both as simply “detection.”
will be no detections over the same time. For there to be no detection at time $T + dT$, there must be no detection up to time $T$ and there must be no detection in the time interval $T, T + dT$.\textsuperscript{17} The instantaneous probability of detection or nondetection depends on search \textit{sweep width} and \textit{search speed} as illustrated in Figure 4.10. It is time invariant. The failure to detect by time $T$ is independent of the failure to detect by $T + dT$. If we let $s$ denote the sweep width in nautical miles, $v$ denote missile speed in knots, and $A$ the AOU in square nautical miles, the probability of detection in the time interval $[T, T + dT]$ is $svdT/A$ and the probability no detection takes place is $1 – svdT/A$. For convenience, we let $\lambda = sv/A$, so that the probability that no detection takes place by time $T + dT$ is $q(T + dT) = q(T)(1 – \lambda dT) = q(T) – q(T)\lambda dT$. Rearranging, we get:

$$
\frac{q(T + dT) – q(T)}{dT} = –q(T)\gamma .
$$

In the limit as $dT \to 0$, we get:

$$
\frac{dq(T)}{dT} = –\gamma q(T).
$$

The solution to this differential equation is $q(T) = a + e^{-\gamma T}$ for an arbitrary constant $a$. Because it is certain that with no time devoted to searching there will be no detection, we have the boundary condition $q(0) = 1$; therefore $a = 0$ and $q(T) = e^{-\gamma T}$. The probability of detection then is:

$$
P_d(T) = 1 – e^{-\gamma T}.\textsuperscript{18}
$$

As depicted in Figure 4.10, $A$ is a circular region. However, the actual shape of the region depends on what the friendly force knows about the enemy submarine’s mission—a priori knowledge. If the Kilo is known to be en route to replace the destroyed submarine, then the

\textsuperscript{17}Because these terms are based on $T$, the “effective” search time, the probabilities are technically “effective” probabilities.

\textsuperscript{18}See Koopman (1980).
A friendly commander knows that the full 360° sweep need not be searched in that it is unlikely that the submarine will reverse direction or veer radically off course. The size of the AOU is assumed to increase with the square of the time elapsed since the last Kilo position update. This assumption is consistent with a circular AOU, or a “pie wedge” AOU (reflecting a priori knowledge of heading limits), or an elliptical AOU with fixed eccentricity (reflecting uncertainties in speed and heading). The effect of knowledge in this case is to reduce the size of the AOU by restricting the search to a fraction of the circle coincident with the direction of the submarine.

The size of the AOU depends on the elapsed time, $t_u$, since the last update and on the speed of the surfaced submarine or:

$$A = \pi \left( \frac{r}{k} \right)^2 = \pi \left( \frac{\omega t_u}{k} \right)^2,$$
where \(0 < 1/\sqrt{k} \leq 1\) is the fraction of the circle that must be searched based on the prior knowledge of the submarine’s route of advance. For simplicity, we ignore the possibility that the AOU will grow during the search. Similarly, we ignore the possibility of updating target data during the search. Now, the cumulative detection probability function becomes:

\[
P_d(T) = 1 - e^{-\frac{s\sqrt{k}^2}{\pi(w^2)}T}.\]

Although the friendly commander has no control over target speed \(i_u\), improved equipment and procedures can greatly affect \(v, s,\) and \(T\) and good intelligence can affect \(\sqrt{k}\).

Figure 4.11 illustrates the increase in detection probability for two cases: when the AOU is 20 square nautical miles and when the AOU is only one square nautical mile. In both cases, the speed of the missile is 450 knots and the sweep width is .25 nautical miles. If we assume that the speed of the target submarine is constant, then the radius of the AOU is dependent solely on the time elapsed since the last update on the target submarine’s location. Note the dramatic difference in the results. For the one-square-nautical-mile case, detection probability reaches its maximum within two or three minutes of search, whereas the detection probability for the 20-square-nautical-mile case has still not reached its maximum after 30 minutes of search.

**Kill Probability**

The probability, \(P_d(T)\), is the probability that the target will be detected by time \(T\). This is the cumulative probability distribution for the density function

\[
f_d(T) = \gamma e^{-\gamma T}.
\]

This function has a mean
This is the expected time required to detect the target. As with times required to collect, process, and disseminate information, a maximum expected time can be determined, and therefore the knowledge resident in the detection time density $f_d(T)$ is assessed as:

$$K(T) = \begin{cases} 
0 & \text{if } \gamma < \gamma_{\min} \\
\ln(\gamma / \gamma_{\min}) & \text{if } \gamma_{\min} \leq \gamma < e\gamma_{\min} \\
1 & \text{if } \gamma \geq e\gamma_{\min}
\end{cases}$$
This can be used to reflect the quality of the target location estimate by influencing the probability of detection.

In general, if $K(T)$ is large—that is, if the uncertainty concerning the remaining search time is small—we would expect a search more effectively matched to the time available. This also has the effect of reducing the search area. If the amount of reduction is $1 - K(T)$, the effective search area, $E_A$, becomes:

$$E_A = [1 - K(T)] \left( \frac{\mu L}{k} \right)^2.$$  

Applying this to the detection probability equation, we get the following adjusted detection probability:

$$P_d^*(T) = 1 - e^{-\frac{s v k^2}{[1 - K(T)] \pi (w r_a)^2} T}.$$  

If we let $p_{K|T}$ be the knowledge enhanced probability of kill, then in this case where a detection is equivalent to a kill with probability 1.0, we get that $p_{K|T} = P_d^*(T)$.

**SUMMING UP**

In this chapter, we have linked the effectiveness of the SLAM-ER against the enemy Kilo to the speed at which the alternative command and control systems and operational networks are able to get a launch platform on station. To do this, it was first necessary to establish adequate measures of effectiveness and performance. Next, we developed mathematical models of collaboration and network complexity to assess the performance of the alternative command and control procedures.

**The Measures**

The paramount objective of the U.S. forces in the TCT vignette is to keep the enemy Kilo from reaching the SLOC north of the island. The JTFC has determined that catching it on the surface and attack-
ing it as early as possible can best accomplish this. The decision to dispatch a launch platform (F/A-18 or UCAV) hinges on the JTFC’s assessment of the time available to him to accomplish his mission. Consequently, the command and control MOP selected for this analysis is *time on target*—i.e., the time available to an attacking aircraft to conduct its attack measured as the time elapsed between its arriving on station and the Kilo submerging.

The combat MOE is *the probability that the aircraft destroys the Kilo given that it arrives on station before the Kilo submerges*. Because of the accuracy of the SLAM-ER (launched from either the UCAV or the F/A-18), detecting the Kilo is taken to be equivalent to destroying it.

**The Metrics**

As with the missile defense vignette, network complexity and collaboration combine to affect combat operations. In this case, however, the decision to attack is based on an assessment about the time required to get an attack platform (UCAV or F/A-18) in position to launch a weapon. The expected latency expression is:

\[
L_{cC} = \frac{1}{1-g(C)} \sum_{i=1}^{\tau} \prod_{j=1}^{d_i} [(1 - K_j(t))^{\delta_i} \frac{\delta_i}{\lambda_i}],
\]

where \( L_{cC} \) represents the expected time required to get the attack platform on station, given the effects of collaboration and network complexity. Complexity is included in the expression \( 1/[1-g(C)] \), and collaboration is a function of the knowledge factor, \( K_j(t) \).

The effectiveness of the operation depends on the probability that the enemy submarine will be detected and successfully engaged. This, in turn, depends on the amount of time, \( T = S - L_{cC} \), available to search and attack, where \( S \) is the time the submarine will submerge. We assume that the SLAM-ER is effective enough that, if detected, a target is assumed to be destroyed with certainty. The MOE therefore is based on the search equation:

\[
P_d(T) = 1 - e^{-\gamma T},
\]
where $P_d(T)$ is the probability that the submarine will be detected in $T$ minutes. The coefficient $\gamma$ consists of the geometrical aspects of the problem, such as the AOU, the sensor’s field of regard, and the sweep width. In addition, it includes the information update frequency from the ISR SSN and the knowledge gained from external sources.