BESA PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

Underwater Internet Cable Cutting: A Neglected Aspect of Cyber Warfare

by Dr. Eado Hecht

BESA Center Perspectives Paper No. 203, April 18, 2013

EXECUTIVE SUMMARY: Cyber warfare is the newest addition to the domain of war. Though attention is usually focused on software aspects of this new battlefield, a low-tech attack on the hardware infrastructure can be much more crippling and long-lasting. Israel is no less vulnerable to an attack of this nature, and increased vigilance by the navy is necessary to prevent it from taking place.

In recent years there has been considerable discussion of the new phenomenon of cyber warfare, its methods, and its ramifications. In essence there are three objectives that can be achieved by cyber-offensive activities: espionage (infiltrating the target's information storage systems and stealing information), denial of service attacks (preventing Internet usage), and sabotage (infiltrating systems reliant on Internet connections and causing functional damage via malevolent programs). The media largely focuses on the use of computer programs as weapons in the cyber domain, but an attack on Internet infrastructure is no less an option for terrorists, and often more devastating and effective. It doesn't require a great deal of computer programming skill to implement, and its effect is widespread and immediate. Even partial success has extensive consequences because of the resultant jamming of traffic on the limited remaining connection.

For example, on March 27, 2013, an Egyptian Navy patrol discovered and arrested three men engaged in cutting an underwater cable connecting Egypt to international internet service. Seacom, the cable operator, said that while the attack was interrupted before the cable had been completely cut, network speed was significantly reduced in Egypt. This was just one of many instances from over the past decade in which cables off the coast of Egypt were cut.

Underwater Cable Cutting

Submarine communications cables convey approximately 99 percent of inter-continental communications traffic, with the remaining 1 percent conveyed with reduced quality and efficiency by satellites. Originally these cables were electromagnetic, but since 1988 have been gradually replaced by fiber-optic cables. Cables have been cut by nature (earthquakes, currents, and even shark bites) but mostly by human-caused accidents (trailing anchors or fishing nets) as well as deliberate military or criminal activity (stealing and selling sections of cable). In fact, damage to cables is quite common, with several dozen up to a few hundred incidents per year. The response to this, in addition to technical improvements such as burying the cables and conducting repairs, has been to manufacture redundancy into the system, allowing for multiple cables to connect to different points by separate routes. This process has been improved by having a number of junctions connecting parallel cables, thus enabling the bypassing of specific sections that have been cut by transferring the traffic *en route* to other cables.

However, there are still weaknesses in various areas of the global layout of the network that can result in a particular client-area being cut off from service or suffering varying levels of service degradation. For example, in January 2008 two cables were cut near Alexandria, Egypt, resulting in a severe disruption of Internet services in regional states. In February 2012, about half of the Internet networks in Kenya and Uganda were cut off from the world. That the more vulnerable areas (Africa, south central Asia, South America) and less vulnerable areas (North America, Europe, east Asia) are in line with the areas' economic status is not surprising; laying and maintaining the cables is extremely expensive.

Targeting international communication cables is not new. On August 5, 1914, the first military action by Great Britain after declaring war on Germany was to send the cable steamer '*Alert*' to cut Germany's five trans-Atlantic submarine telegraph cables. Similar actions by other British ships cut other sections of Germany's international telegraph communications with the rest of the world. To communicate with its embassies, colonies, and naval bases around the world Germany was forced to rely on other means, specifically the telegraph services of neutral states. However, most of the non-German cables connecting Europe to the rest of the world had to pass through a British relay station and were thus vulnerable to eavesdropping. This had a major strategic effect on the conduct of the war, when in January 1917 the British intercepted and decoded a telegram from the German government to the Mexican government proposing that Mexico should declare war on the United States. The Germans hoped that fighting with Mexico would keep the United States

from involving itself in the war in Europe. This telegram, known historically as the "Zimmerman Telegram," was one of the catalysts for the US declaring war on Germany in 1917.

The Challenge for Israel

Until recently Israel had only one major cable connecting its Internet to the world; thus every malfunction immediately impacted on Israel's economic and private use. Redundancy was achieved only via satellite communications, though well below the requirement. Though today there is a second parallel system which provides sufficient protection from natural or accidental incidents, a deliberate attack – similar to that of the British Navy on Germany's telegraph network – has a simple target. These cables require active protection measures if Israel is to prevent severance from the international Internet. In 1914 the British attack mainly affected Germany's diplomatic and military capability, and Germany had sufficient, if vulnerable to eavesdropping, alternatives. Today, the diplomatic and military effects of having Internet communication with world at-large cut off would be negligible, but the direct and indirect economic consequences could be extremely expensive to Israel's economy, especially with the transfer of much data to online cloud services that are actually placed abroad.

Defending against the new threat means adding a new mission to the Israeli Navy; however, there is no need for vastly increased naval resources to fulfill this mission. The Israeli Navy has for decades been monitoring the activity of vessels in Israel's vicinity for potential terrorist activity, and the navy recently beefed up its security capabilities to protect its new maritime gas-production facilities from various terrorist and military threats. Therefore, the important factor is increased awareness and adapting existing maritime surveillance to ensure that the Internet cable routes are properly covered as well. A secondary necessity is a rapid repair capability, which is in any case the purview and interest of the cable companies themselves and only needs government supervision and naval escort (in times of war) to ensure a swift response.

Dr. Eado Hecht is an independent defense analyst specializing in military doctrine and its interpretation. He teaches military theory and military history at Bar-Ilan University, Haifa University and at the Israeli Defense Forces Command and General Staff College, and serves on the Editorial Advisory Panel of The Journal of Military Operations.

BESA Center Perspectives Papers are published through the generosity
of the Greg Rosshandler Family