An Information Revolution in the Middle East?

Ariel T. Sobelman

Recent wide-spread publicity in the Israeli and international media regarding a young Israeli computer hacker's penetration of classified Pentagon computer systems has raised public awareness of crime and terrorism in Cyberspace and the Internet. The youngster, Ehud Tennenbaum, managed to dismay computer security experts worldwide and to mobilize the police and justice authorities, both in Israel and the United States, who tried to contain the alleged damage he caused. In his defense, Tennenbaum claimed that he simply wanted to send an "elegant" message to the power figures in the Pentagon by breaking through their computer defenses. Thus, the phenomenon of a modern day Robin Hood, or Cyberspace-delinquent – Tennenbaum's case being the most recent in a long list of youths penetrating government, economic and military systems – illustrates the extreme vulnerability of computer-driven systems. Tennenbaum's prank was a powerful illustration of the establishment's helplessness in face of such attacks. The degree to which our lives have grown to depend on computers and other information-reliant infrastructures, and the apparent ease with which these critical infrastructures can be sabotaged or paralyzed, provide yet another warning of one of the main hazards of the "Information Age."

To the public, the threat of hackers and the vulnerability of systems and infrastructures connected to the Internet and other communication systems are a relatively new development. However, security experts and defense planners worldwide (particularly in the United States) have, for several years, been exploring the implications of the introduction of computers, the Internet and other forms of information-intensive media for all aspects of life – from academia, through commerce and government to the military. Assuring the unobstructed flow of information through our vital pipelines of life – civilian and military – has become essential in securing national security and national fortitude, and the term "information warfare" has been adopted by the U.S. Department of Defense to describe a huge spectrum of information-age threats.

Indeed, information warfare has become one of the most intriguing, albeit least understood, topics on the international security agenda in recent years. Information warfare is perhaps best defined as the operational product of the information revolution. It includes all possible efforts to deny, exploit, corrupt, or destroy an adversary's information system, while protecting oneself against the same. At the end of the 20th Century and the dawn of a new millennium, the world is shifting out of the industrial age and into the information age – the third-wave civilization, where information and other forms of fluid knowledge take over as the most valuable commodities and become strategic assets. Therefore, a nation's ability to both produce and utilize information and to protect its information assets becomes synonymous with securing its national security.

In the military realm, the conundrum of information warfare is engaging the attention of theorists, national security planners and military apparatuses in many countries. Unfortunately, our understanding of information, at both the operational and strategic levels, is impeded by a poor understanding of the hybrid nature of the marriage between the seemingly unrelated computer/information age and the art of waging war. It is impossible to understand activity on the "information front" in the Middle East without first highlighting some technological and philosophical changes that have contributed to forming our perceptions of national security in the information age, and the many ways in which military organizations are transforming and re-organizing to adapt to this new environment. For it is from the interaction between a new technology and strategic vision that military innovation occurs and a new form of warfare is created. Once we have a better appreciation for the technological aspects of the information revolution, as well as the conceptual patterns of progress, it becomes easier to approach the emerging field of information warfare.

Over the last decade or so, the United States and other Western societies have approached military dilemmas related to the information age very similarly. Their logic stems from common foundations: they have evolved into the information age organically, from the bottom up. Fascination with the networked world and the constant introduction of ever-faster computing capabilities, including the ability to process, exchange and disseminate large volumes of information in real-time, had a dramatic effect on virtually every aspect of life. The military,

the economy and government have become increasingly information-technology-reliant and are losing the ability to function effectively without them. But vital information-reliant infrastructures and assets are vulnerable to computer hacking. In an information-age society, widespread damage to vital strategic information assets can bring an entire country to a standstill and paralyze the military's ability to operate. Thus, the information age is reshaping the ways in which strategic assets are viewed, and information warfare highlights how we perceive threats to these assets and to national security.

Information Warfare (IW) Characteristics: Selected Middle Eastern Countries

	Internet Hosts 1998 (approx)	Super Computing capabilities*	IW vulnerability*	Potential IW capabilities*
Israel	65000	yes	very high	very high
Iran	unknown	probably	moderate	moderate-high
Kuwait	6500	yes	moderate-high	low
Jordan	300	no	low	very low
Egypt	3500	yes	moderate	moderate-high
Syria	unknown	no	low-moderate	low

*Author's assessment.

A number of models were recently proposed for examining the relationship between the information age and its effects on military organization. Some of these models view the challenges through a technological prism and suggest that digitizing the military will serve as a force enabler and multiplier. Other models envision the information-age military as a product of an epistemological process – that is, a mental change – beyond the purely technical realm of providing new technologies to the war-wagers. Such an information-age military construct would, from a doctrinal point of view, be radically different from a merely digital force that would implement technological breakthroughs but not embed the information-age mentality into its understanding of national security or into its operational doctrine.

In the United States, the Army's Training and Doctrine Command (TRADOC) was tasked to address these dilemmas by designing and testing possible future force structures that would integrate and incorporate the latest information technologies and best produce information for the wagers of war. TRADOC's approach hypothesizes that providing the units with superior capabilities to process, exchange, utilize and protect their information will serve as a significant force multiplier. Inter-connecting these capabilities throughout the force and operating under a protective umbrella of information dominance may produce a new form of warfare for the information age.

Consequently, TRADOC began a series of war-fighting experiments to test technologies and doctrines for the future American ground forces at all echelons – from task forces to corps level. The FORCE XXI Advanced Warfare Experiment (AWE) series is by far the most impressive extravaganza of technology. Aside from an unprecedented array of high-tech gadgetry for war-fighters, it has introduced a barrage of information-age terminology. The digitization of the battle-space is consistent with the first model described, in which superior information technologies lead to the strategic summit of information dominance. This dominance will, in turn, contribute to an increase in lethality, survivability, sustainability and tempo across the force.

However, is Force XXI really a genuine product of the information revolution? A second model suggests that the digital approach alone fails to take into account the most important dimension of change. Force XXI may have digitized the battle space and enhanced the forces' situational awareness and visualization capabilities, but it has not taken the conceptual leap to produce a truly new military doctrine that integrates the dramatically different ways in which we perceive threats to national security with the technological opportunity to generate a new form of warfare.

IW in the Middle East

How is the Middle East affected by the information revolution, and to what extent is the region undergoing changes and processes similar to those in Western societies and militaries?

While the information revolution has traditionally been associated with the Western world and open societies, in the past two years there is growing evidence that the Middle East has also come under its influence. Several countries in the region have started exploring its implications for their national security in general, and to harness the power of information at the operational level. The levels of investment in information technologies in several Middle Eastern countries, and the extent of progress in information-utility, will bear directly on Israel's national security policy in the next several years and affect Israel's ability to maintain a technological edge over its

adversaries in this new dimension of the battle space.

Most countries in the Middle East were introduced to the information revolution later than Western countries. The patterns of explosive and rapid development are significantly different from the evolving nature (at least in the early stages) of the Western information revolution. This is true both of national security perceptions, in general, and of military information capabilities, in particular. Over the past few years, we have witnessed in the Middle East a giant leap forward: large investments in computing facilities and communications infrastructures (leading to rapid progress); a growing presence on the Internet's World Wide Web; and a growing internalization of the correlation between the information age and national security.

In Egypt, for example, there are many indications of a comprehensive effort to create a national information infrastructure that will serve both military and civilian needs. The zeal with which Egypt is approaching its information project, presenting it as a monumental national venture, is indicative of the deep-nested understanding of the relationship between the information age and national security. The civilian dimension manifestation is evident in the concentrated and costly efforts to create a national information infrastructure, which the Egyptians perceive as vital for developing their ability to play a role on the international information super-highway. From the Egyptian perspective, the Internet is a tool of dual use in its purest sense, serving both civilian and military purposes. The gathering of open-source intelligence is the most common example; the Internet has magnified access to unprecedented amounts of information at virtually no cost.

To illustrate the extent of change, consider the following figures: In 1993, Internet services in Egypt were carried through extremely low bandwidth fibers with a capacity of 9.6 Kbit/second (a BIT is the basic unit for measuring data traffic through a network, and K stands for a thousand), with less than 2000 people using the Internet in all of Egypt. By the end of 1997, however, more than a dozen companies were providing Internet services to academic, business and government users, with efficient connections to European and U.S. networks. All universities are now connected, as are more than 30 government ministries and organizations. In the commercial sector, from barely a dozen just a few years ago, there are currently well over 10,000 companies and firms conducting commerce and trade through the Internet. Egyptian military efforts are less well known, but the careful Egyptian examination of the American Force XXI process, together with their known steps to establish a military information branch, military C4I (Command, Control, Communications, Computing & Intelligence) capabilities, and information operations units (special units with highly trained hackers), are highly indicative of the future direction.

Other Middle Eastern countries are advancing in a similar direction. Extensive national investments in digitization, information infrastructures and technologies potentially useful for military applications all indicate that the region is rapidly moving into the information age and may become highly potent in information warfare in the not-too-distant future. The American military, in their futuristic war games series associated with the Force XXI process, make quite alarming estimates and projections of future information warfare capabilities likely to be available to a number of Middle Eastern countries, including Iran and Iraq.

The Middle Eastern top-down approach to the information revolution (in contrast to the bottom-up, natural development process experienced in the West) and the rapid progress made in this region raise a plethora of questions that need to be studied in order to gain a better understanding of what the region may look like in the information age. Countries investing in information warfare capabilities, as well as the circumstances in which information warfare may be employed in the region, must be identified.

There are two important factors that Israel must consider when addressing the challenge of information warfare in the Middle East. First, in this high-tech world, Israel's ability to maintain an edge over its adversaries will change significantly. The basic time unit that we have traditionally used to measure a technological advantage is shrinking drastically. After all, in Silicon Valley, the term "generation" is defined as roughly 14 months. Being accustomed to a several-year technological gap between us and our neighbors, we will find that our advantage in information warfare technologies is eroding much faster than we expect. Israeli security policy must take this into account.

Second, as a result of the fundamental changes in the nature of technological progress and of the previously described developments in the Middle East, Israel may find itself facing much more advanced information warfare capabilities and much greater vulnerability than it expects. In the final analysis, the extent to which future Middle East conflicts will be affected by information warfare is an open question. But the fact that they will be affected is not.