CYBER –

THE FIFTH DIMENSION

Yair Cohen[1]

Intruduction

The "Cyber" that recently burst, with great intensity, into public discussion and global consciousness, is not a new entity. In its basic components it has existed since the first computer started storing data that another agent might be interested in having or in disrupting. It has existed since the first command and control system was activated, which turned the advantage of centrally-controlled critical infrastructures into security challenges and potential points of failure. The fundamental change is, the intensity of damage cyber attacks can cause and are already causing today, in both the military and civilian areas, as one.

On the military level, introduction of Cyber Warfare into the battle space can be resembled to the revolution that took place on the battlefield with the introduction of aircraft, at the beginning of the last century. The potential future destruction concealed within it, will be equivalent to the most lethal of physical weapons.

Therefore, cyber should be regarded as the fifth warfare and defense dimension after: land, sea, air and space.

[1] General (ret.) Yair Cohen had 32 years of Military Service in the IDF. At his last position he served as the Head of the Cyber & Intelligence Unit.

On the civilian level, the main target for using cyber weapons are vital and critical infrastructures.

Cyberspace entails a vital infrastructure in itself, being the operational basis on which all the country's essential arrays and infrastructures are established.

Infrastructure is defined as vital when its disruption can cause economic and social crises with political, strategic and security implications, which will undermine state foundations and global stability.

Every day we witness repeated attacks aimed at financial theft of huge sums, theft of confidential information such as intellectual property for competitor use, damage to or disruption of infrastructures such as electricity, gas, water, communications and computing, and a gross intrusion into the confidential and intimate data of countries, organizations and individuals.

According to data from the Israeli Check Point company, as of mid-2011, about 300 million cyber attacks occur worldwide per second.

A substantial portion of these attacks are strategic attacks, in respect to the damage caused to the most sensitive security organizations and the country's vital infrastructures.

The economic damage of this cyber aggression is estimated at billions of dollars while more remains concealed than known.

Cyber brings to a peak the asymmetric dimension within which a marginal agent, in terms of its real force, can achieve a critical impact against a highly powerful agent.

The enlightened civilized world has encountered a dark international force of terrorism, crime organizations and states, for which international law and norms do not exist, with unbridled hackers joining them, driven by myriads of interests.

And we have to admit that currently there are no tools available for proper response at local, state and certainly the global level, in a world where one country's vulnerability brings about serious consequences for most of the others.

The "Butterfly Effect", true at the state level, in which the impacting of one infrastructure leads to an escalation in the impacting of other infrastructures, has also an identical effect on the global level.

For instance, and as has already happened, cyber attacks on global stock markets or central banks will result in chain-reaction damage in the global financial system.

Cyber Warfare complexity stems from the blurring of several areas that were clear and defined in the conventional warfare world, which was familiar till now.

I'll mention three of them:

(1) The first element is the difficulty in the unique identification of the attacker

(2) The second element is associated with dissolving the demarcation existing between actual combat situations and non-warfare situations, regarding states in conflict.

(3) The third element lies in the significance of cyber attacks in the civilian and security sectors and the dependence between them.

Difficulty in the unique identification of the attacker

As a rule, even a cyber attack by an average hacker, who is not interested in disclosing his activity, which was intended for intelligence purposes, theft or planting malware, is not easy to detect, following an absolute determination that this is not a technical fault. Let alone when it comes to professionals, who for their intrusion detection, special tools and skilled people are required.

Furthermore, even if the attack was identified, it is even harder to identify its source when the attacker makes use of technologies and tools for maintaining anonymousness, which enable him to be camouflaged behind servers of various countries.

We have here a divergent from all existing forms of warfare in which the attacker identity is revealed almost certainly after the attack, as it requires physical arms reaching the target.

Cyber allows, for the first time, to attack quality targets without reaching them physically, and without the need to face defensive forces and be exposed, later on, to a responsive action.

The deterrence element, which was a warning sign even for terrorist and crime organizations and certainly for countries, is obsolete and does not exist today, regarding cyber weapons use.

Hence, even the direct response capability to a cyber attack, whether by computerized attack or physical response, is most problematic both technically and regarding legal policy.

The concealment phenomenon may also have far-reaching consequences of manipulations, where the attacker side will have, in fact, an interest to cause friction between different organizations and countries by creating a false impression regarding the attack source.

Such global conflicts may break out when 'combustible material' ignites from the match lit by a manipulated agent, who benefits from the inter-state conflict he brought about.

Dissolving the demarcation existing between actual combat situations and non-warfare situations, regarding states in conflict.

The second element is associated with dissolving the demarcation existing between actual combat situations and non-warfare situations, regarding states in conflict.

As a result of the above mentioned, even a situation of peace and/or consensual non-warfare between confrontational states, might become an active battle scene under a cyber-mist disguise.

Cyber weapons allow undertaking, in a consensual non-warfare situation, of offensive action that so far was undertaken only in an open and declared war, in which its security or economic damage on the opposite side is very severe, without the risk of public exposure. Therefore we regard the cyber threat, in many similar ways, as we regard our preparation for war on global terrorism.

The statement of George Orwell in his book "1984" is particularly relevant to the cyber area: "Even the word war is deceptive. It may be said that war once it became endless, has ceased to exist. So war is actually a kind of a peace."

Significance of cyber attacks in the civilian and security sectors and the dependence between them.

The third element lies in the significance of cyber attacks in the civilian and security sectors and the dependence between them.

Naturally, physical bombardment of vital civilian infrastructures has a direct impact on the functionality of the military.

However, the relative ease of using cyber weapons increases the extent of destruction, to another level.

A cyber attack planned with the appropriate attack tools may strategically disrupt an intrastate system by simultaneously impacting both civilian and military systems functionality. Functionality of the military program that was designed to achieve a decisive battlefield advantage depends directly on the continuation of the civilian systems functionality for supplying electricity, water, transport, and communications and so on. Therefore, even if we assume theoretically that the army would be completely secure against a hostile cyber intrusion, it still needs the same immunity of civilian systems, to which it is connected, via an Internet connection with a large number of channels and links.

Therefore, Bruce Schneier's conclusion in his article about the quantum encryption is correct, saying that "The strength of our information security is as strong as the weakest link in the system".

We therefore need to resemble the cybernetic battlefield to the kinetic battlefield where virtual attack and their defense weapons, replace physical attack and their defense weapons (Figure 1).

What is required therefore, as a means of coping:

Like many things, dealing in the cyber area also requires at all levels – "cybernetic steering", in the initial and original sense of this term.

Steering at levels of the individual, organization, country and the civilized world of which normative and legal integrity is the guiding light.

A comprehensive and integrated defense concept at the state, army, organizational and vital infrastructure systems level, should be adopted.

The existing reactive defense concept providing local security solutions, as good as they may be, is not sufficient anymore, and those who will keep insisting only on it, their infrastructures may soon collapse.

In any case, the specific security solutions will continue being the critical building blocks in the overall defense array.

The reactive defense approach against computerized intrusion should vary conceptually and operationally and be replaced by a proactive defense approach.

The new defense concept should continue to prevent hostile intrusion, but once such intrusion occurs, it should alert, identify the attack source and respond to it, share the information with other agents and provide full operability by immediate activation of an alternative solution.

It is necessary to establish a command and control center to store information from vital computer networks continuously and for the long-term, to obtain a cyber situational picture, enabling ongoing management in routine or emergency situations.

The Cyber Center will include technological and operational capabilities in the analytical cyber intelligence and research areas.

Advanced simulation tools will allow examining the local and global impact of an identified attack and training the defending cyber personnel, on how to deal with expected threats.

Automated tools will allow cyber policy enforcement and monitoring in vital networks (Figure 2).

Constant cooperation is required between the security sector, intelligence community, industry, and hi-tech companies and academia. Israel is a pioneer in generating such cooperation.

For global coping, it is vital to strive toward international cooperation and impose local liability on the countries, not only to prevent the attack on them but also from them.

An effective deterrent dimension should be generated in the cyber world in which it will be clear for the side attempting to execute a hostile attack, that the price he will pay for this attack bears far-reaching consequences for him and his country.

Given appropriate technology tools for attacker identification, the legal plane in the international scene will also gain practical effectiveness, which is insufficient today.

The State of Israel has been investing for several years in the information security and cyber warfare area as an integral part of the military and national defense strategy. The Security and intelligence community in Israel having understood for several years the potential threat on one hand and the opportunity on the other hand, invests a lot in the field, and has even reached breakthrough achievements.

Research and academia, involving tens of breakthrough hi-tech companies, focus on the cyber area in developing qualitative solutions designed to prevent and anticipate the hacker technology.

At the same time, the Israeli Defense Industry has developed comprehensive cyber solutions expressing an integrative concept at all levels of technological and operational capabilities.

In conclusion - the virtual world of science fiction literature is here and now.

Cyber - no more a security issue, but a national security issue!

No longer a national security problem applying to a single state, but a global security problem!

And this requires a new countering concept and an improved deterrence balance, to ensure the proper functioning of the world we live in.