Cyber weapons against the power industry

by Vladimir Gurevich, Israel Electric Corporation

Recently there have been a lot of articles on the new reality of cyberwars in cyberspace published on the Internet and in the mass media, some of which are quite inflammatory.

For example, the author of article [1] says: "the first cyberwar has already been launched: it was triggered by the governments of USA and Israel against Bushur NPP in Iran".

The underlying concept of the "cyberwar" was disabling of centrifuges through interruption of the operation algorithm of speed controllers. It was the aim, according to the claim, of the Win32/Stuxnet worm located in centrifuge operation controllers at Natanz plants. Initially the virus had nothing to do with the Bushur Electric Plant despite numerous speculations on this subject. Another matter is that other complex systems are also exposed to virus attacks and first of all it is referred to automatic systems operating the whole plants and metropolitan infrastructure, including public water supply and power supply systems.

By changing the programmable logic controllers' (PLC) code the virus tries to reprogram controllers of industrial systems to get control of them under the table. According to some data, everyday this virus makes several thousand attacks on controllers. We think that this should be noticed by the technical community and first of all by power industry managers. Moreover, this dangerous virus has already infected controllers of power systems. In 2009 the US government admitted the detection of a virus capable of disabling power plants in the country. The real issue is the shift of smart grid vulnerability to hacker attacks.

In fact, if all elements of the smart grid are controlled by commands through the networks with TCP/IP protocols, there is a huge risk of external intervention to the power system operation. Many experts emphasised this hazard devoting international conferences to it. Only apologists of the smart grid, for some reason, "do not notice" these problems. What do we hear from the apologists of the smart grid? Nothing but usual reservations about the necessity to isolate the internal network of the smart grid from the external web (this concept was realised in Iran), about access passwords and other trivial safety measures. We all understand that all these measures can limit access for normal people, but not for experienced hackers cracking even the very well protected networks of the Ministries of Defense and banks.

Fig. 1: The first cyberwar was claimed to be launched against the Natanz plant in Iran.

However, hackers are not the major concern since the armies of many countries of the world have special divisions consisting of skilled professionals intended for cyber wars, that is, for cracking and sabotaging the protected computer networks of the enemy. It is safe to say that the computer network of the smart grid will be the number one target for such divisions. "Welcome to XXI-st century war," says Richard A. Clarke, former Special Adviser to the US President George Bush for Cyber Security and National Coordinator for Security and Counter-Terrorism, "Imagine the bursting electric generators, the derailing of trains, the crashing of planes, the blowing up of gas pipelines, the arms systems suddenly ceasing to work, and armies which do not know where to move". This is not an episode from the next Hollywood blockbuster it is a summary of the consequences of the new type of battle conducted as cyber war by skilled American experts.

Americans have been the most active in this area. In October 2010, the US Cyber Command, under the command of Gen. Keith Alexander, started its operations. Being a part of the top secret National Security Agency (NSA), the organisation has united all previously existing cyber safety departments of Pentagon. Even now Cyber Command has about 1000 employees, but the military has already announced the initiation of a major hiring plan for particular specialists. Some of them will be in charge of protection of military and state infrastructures as well as of the most important commercial properties of the state. This was announced on the eve of the US Cyber Challenge program initiated early in February and aimed at finding 10 000 young computer geniuses [4].

The current Head of Cyber Command of the Pentagon, General Alexander has declared at hearings of the Military Service Committee of House of the USA that the effect of cyber weapons is comparable to the effect of mass destruction weapons. Meanwhile, cyber weapons are being developed at a rapid pace. Many countries – including the US, Russia, China, Israel, the UK, Pakistan, India and North and South Korea – have developed sophisticated cyber weapons that can repeatedly penetrate and have the ability to destroy computer networks, cyber-security specialists say, write Siobhan Gorman and Stephen Fidler, authors of the article [5]. Some representatives of the American intelligence and analysis are afraid that a cyber weapon can fall into the hands of terrorists. "The question is: When will these leak to al-Qaeda?" said James Lewis, a cyber-security specialist at the Centre for Strategic and International studies who regularly advises the Obama administration. [5]

Additionally, one of the former employees of NSA, Charles Miller, has even calculated that the creation of a cyber structure capable of successfully attacking and completely paralysing the USA would cost only $98-million [5]. "We consider it as one of the basic perspective directions and expect two order growths of the market totaling billions dollars," emphasised Steven Hawkins, Vice-President of the Intelligence and Information Systems Division of Raytheon. It is a highly lucrative business in that the cyber budget reached $8-billion this year, and to 2014 this amount will grow to $12-billion. While the annual increase in the budget expected for other directions will come to 3 – 4 % in the short term the rate for cyber safety will grow at least 8% annually. The leading role in this new type of war will belong to military men, and naturally they will receive the lion's share of the cyber budget: more than 50% out of $8-billion in 2010 will be given to the Pentagon.

In 2011, USA plans to embrace a doctrine of cyber safety. Its aims were revealed in a policy paper by Deputy Defense Secretary William J Lynn III under the symbolic name "New Space Protection". The main idea of the article is that from now on the USA considers cyber space as the potential battlefield along with land, sea and air. In parallel, NATO has started to work on the development of a collective cyber safety concept. At an Alliance Summit held in November 2010, it was decided to develop an action plan for cyber security. The document should be ready by April 2011 and signed in June. The main concept of the document centers around the creation of a NATO cyber accident response centre. According to "Kommersant" Magazine, initially the centre was planned to be commissioned in 2015 but on the insistence of the USA the term was reduced by three years.

The paralysis of control systems, major outage of whole power systems, chaos in air and land transport control systems, interruptions to bank stock exchange systems, disconnection of Internet and cellular phones are all in the scenario of cyber war in American apologist's opinion.

The situation is dramatised by the fact that up-to-date technologies enable developing chips or writing special secret commands to control program of microprocessor-based electronics, which destroy the equipment on receipt of a certain signal. Responsible microprocessor-based electronic control systems can no longer ensure full protection of industry and power systems under every circumstance and, even worse, can damage the equipment under control as it happened in Iran.

Any international agreements on limiting cyber weapon use (such as proposed by Russia, but declined by USA) will never be effective since it is not possible to control their fulfillment. So what is left to do? We need to assess not only the advantages of modern technologies but thoroughly analyse the consequences of wide spreading such technologies, soberly estimate potential hazards, especially in such sensitive and important field as power industry, as well as timely development of measures for preventing intentional damage and restoring damaged systems.

References

[1] Fredric B Cyber, Wars of XXI Century. – Power Systems and Industry of Russia, 2011, No.3 (167).

[2] V I Gurevich, Smart Grid: New Prospects or New Problems? – Electrotechnical Market, 2010, No.6 (part 1); 2011, No.1 (part 2).

[3] V Scherbakov, Virtual Space, Real War. – Military-Industrial Courier, No.40 (356), 13.10.2010.

[4] A Usov, USA and NATO Mobilize 10 000 Young Hackers. Cyber Armament Race is a New Hobby of Pentagon. RIA Noviy Region, February 15, 2011.

[5] S Gorman, S Fidler, Cyber Attacks Test Pentagon, Allies and Foes. – Wall Street Journal, September 25, 2010.

Contact Vladimir Gurevich,
Israel Electric Corporation,
vladimir.gurevich@gmx.net ❖