CYBER SECURITY: THE PROBLEM OF THE 21st CENTURY

Dmitry Vavrovskiy

Saint-Petersburg State University of Aerospace Instrumentation,
Saint-Petersburg, Russia

Dima_vavrovskii@mail.ru

I. INTRODUCTION

Computers play a big role in our lives. None organization, none house nowadays can't do without these devices. With their creation, wide horizons of prospects became opened for mankind: computers made various operations simpler, they allowed us to model and automate different processes, make calculations far much faster, increased efficiency of the whole systems. The majority considered computers as a part of our future. However, some people saw new potential threat in wide capabilities of digital equipment. And these fears were justified: hacker attacks, cracked accounts and websites, stolen passwords, disabled and even damaged computers – all these things became real and any of us certainly faced them even once in life. And what if a computer contains not private files, which loss is not critical, but serious secret information, which disclosure can lead to unforeseen consequences, cause troubles to a whole organization's work, or even could give cause for a war?

II. REAL THREAT FROM VIRTUAL WORLD

So, can we speak seriously about the danger of computerization? Taking into account the interest of world community in this problem during recent years, the answer is yes. Not so long ago, in 2009, Dr Hamadoun Touré, Secretary-General of the International Telecommunication Union during Geneva Forum opening announced, that it is cyberspace where the Third World War could start. Indeed, anyone, who has much knowledge in computer technology and programming, can seize power and assemble a virtual army of infected computers (so-called "bots"). In addition he said, that, as we can learn from conventional war conflicts, the best way to win is not to start [1].

Over 20 conferences devoted to computer systems security are held annually, and in November, 2010, in EU occurred so called Cyber Security Exercise. Specialists simulated global hacker attacks on critical elements of management system and developed defense methods for such attacks. In USA, by the way, similar practice is common – in 2006, 2008 and 2010, special services imitated an attempt to break up communications and embed into link channels between government structures.

In 2009 USA President Barack Obama established special cyber security department and personally appointed so called "cybertsar" – the one who is responsible for computer crimes in the country.

Famous analytics, looking ahead, warn us about other, not so obvious, threats. Russian futurologist, specialist in technical forecasting area, honored president of International Futures Research Academy Igor Bestuzhev-Lada once was interviewed by Vladimir Pozner, and he suggested, that the main threat of the 3rd millennium is attempts to recreate a man using new cutting-edge technologies and potential displacement of ordinary humans by such "enhanced people", or cyborgs [2]. Artificial heart is already created, also there are experimental attempts to create lungs, eyes and other parts of body, so we already can treat seriously to such statements.

III. CYBER THREATS DETERMINATION

Unfortunately, there is no single document defining the essence and concept of cyber threats. One case, if hacker attack was aimed at stealing money from credit card or bank account of some person, or, for example, it was done to sabotage some organization's work. Other is when criminal actions were committed to cause harm to an ethnic group or even to undermine constitutional state system. How to distinguish the concepts "Cyber attack", "Cyber crime", "Cyber terrorism"?

As we can see, besides of the computer cracking itself, other, not connected with computers, factors are also important, like personality, intentions and political motivation of a criminal. We can give an example of Vitek Boden, native of Australia, who in 2000 year broke water systems of Maroochydore and poured polluted sewage out into urban water supply, with intentions to get a job in water conduit cleaning.

His actions were not considered as terrorism, still, if one man could do this, what can prevent organized terrorist group from doing the same?

In whole, “Cyber crime” can be defined as a crime more or less involving computer, either as a means or as a target. And it is not necessary should be committed using program methods, physical action is also included into this category. If you want to define an act as a “Cyber terrorism”, besides above-listed, political motives should also take place. In addition, there is another opinion, that there can’t be such concept as “Cyber crime”, because it is an ordinary crime, and cyberspace is just a place where it was committed or means, with the help of which it was committed. In that case we can consider Julian Assange process as a significant one. He is the creator of Wikileaks website, through which top secret information, concealed by different states, “leaked”. The case hasn’t finished yet, but no matter how it ends, the precedent itself will be considered as historical and its result will considerably influence on other similar cases.

IV. ECONOMIC CONSEQUENCES

To analyze cybercrime problem more widely, it is necessary not to just identify it, but also to evaluate the incurred losses. According to Unsecured Economies: Protecting Vital Information 2009 report, during 2008 businesses lost more than $1 trillion due to data theft and cybercrime [3]. Enormous money. World GDP, according to World Bank, is $70 trillion for the same year [4].

Also we should take into account American Computer Security Institute’s “Computer crime and security survey”. About 500 companies took part in the survey, and in 2009 annual loss from cyber crime is at average $234 thousand per company. Of course, the sum is not so big, but it is also not so small, besides, it is the result of several years’ preventive work. The peak of losses was in 2001 – companies reported about more that $3 million loss. Then it was steadily decreasing. In 2006 the indicator fell to $168 thousand (this is the lowest value ever), however, it doubled up to $345 thousand next year. The most “popular’ threat in 2009 (and it have been taking first place for already 5 years), traditionally, is malware infection – over 64% of respondents faced it, the next one is theft or loss of mobile hardware with valuable data (42%). 34% reported that their computers were used as senders of phishing messages. 29% were subjects to Denial of Service attacks. If we look at all rates during the last 5 years, we can see, that the correlation didn’t change much, so we can say, that hackers still use the same variety of attack means, and don’t give preference to only one type [5].

According to the report of Internet Crime Complaint Center (FBI department, which is responsible for internet crimes), the amount of complaints received in 2009 increased by 22,3% compared to 2008 and consisted 336 thousand (overall loss is $560 million against $265 million in 2008). During the last 5 years, the amount of complaints and losses was growing steadily [6]. And, of course, we should realize, that the official data is always lower than the real number of internet crimes.

V. CONCLUSIONS

Nowadays, information and data theft have become one of the most serious global problems. Interest from worldwide community to cyber security matter confirms that the problem exists, losses from illegal actions, connected with computers, are still quite big. Unfortunately, it is very hard to stop it and other illegal actions, connected with computer, because in response to every new defense method new program and hardware means are created. And also, one of the weakest links in this chain is human factor.

Not so long ago, in January, under the aegis of World Economic Forum, “Global Risks 2011” report was issued. Cyber security was included in a list of daunting problems of the nearest future. Authors analyzed and determined 4 distinct global risk-related activities: Cyber theft, Cyber espionage, Cyber terrorism and even Cyber war [7]. Vital government objects are connected using computer networks, programs control production processes, plane autopilots are responsible for our security – so, cyber threats are closer, than we can imagine.

At the moment attention to cyber security is very high. The problem is accepted, different measures are been developed, a great deal is done, but still much more is need to be done.

REFERENCES

[1] http://www.computerworlduk.com/news/applications/16938/next-world-war-could-start-online/ - Computerworld UK, Next world war could start online, By Peter Sayer | IDG News Service | Published 12:09, 06 October 09

[2] “Pozner”, issue 69, 21.11.2010, Channel One (ORT).

[3] http://resources.mcafee.com/content/NAUnsecuredEconomiesReport - McAfee Unsecured Economies: Protecting Vital Information

[4] http://databank.worldbank.org/ddp/home.do - World Databank

[5] http://pathmaker-group.com/whitepapers/CSISurvey2009.pdf - 14th Annual CSI Computer Crime and Security Survey (2009)

[6] http://www.ic3.gov/media/2010/100312.aspx - IC3 2009 Annual Report on Internet Crime

[7] http://www.weforum.org/reports - World Economic Forum, Global Risks Report 2011