Systems Research & Development

A Systems Defense Series

Current Methods of Cyber Defense

By

Alice Savitsky

2011

Contents

Introduction

The Paper offers excerpts from *The Conceptual Model of the Information Network Impenetrable for Cyber Attacks* (Part 1. Current Methods of Cyber Defense).

The supporting data and information were obtained at the open for general public websites. In full version of the Paper, references to sources mentioned in the text include the URL and title of web article.

The Conceptual Model of the Information Network Impenetrable for Cyber Attacks was developed because, presently, there is no information network, which is invulnerable to cyber attacks: the attackers can access, control, and assimilate any existing information network; data within any existing network can be accessed, modified, transferred, and destroyed without permission or knowledge of the data's creator/operator/owner.

The idea of information network impenetrable for the cyber attack is neither evolution nor improvement of existing systems; it is a new concept.

Theoretical basis is the general systems theory.

The implementation of the proposed *Model* will

1/eliminate the problems resulting from unauthorized access and theft of research and other data and information, which the current information networks and services are not able to prevent

2/ allow development of a new strategies of information and knowledge creation, transmission, access

3/ allow creation and maintenance of a new market for the data–information–knowledge technologies and services, which sustain evolving systems

4/ provide unprecedented strategic and market advantages for the owners and users.

The *Conceptual Model of Information Network Impenetrable for the Cyber Attack* contains a description of

a/ principles of operation

b/ components and processes

c/ some additional technological innovations needed for implementation; however, at the current level of technological development, there are no restrictions, which would preclude implementation: all components exist or can be assembled, written, developed, integrated, and manufactured

d/ the general operational cycle of the technologies and services created on the proposed *Model*.

The information networks, information technologies and services based on the proposed *Model* will be capable of sustaining the impenetrable for the cyber attacks and evolving systems (financial, research, and the others).

Part 1. Current Methods of Cyber Defense

Executive Summary

Part 1 contains brief analysis of the current methods of cyber defense, which lead to the following conclusion:

The current methods and strategies of cyber defense are based on the classical strategy of failure: ***response***, and only if and after the attack is detected and the attacker is identified. If the attacked system is not able to identify the attacker, it unnoticeably comes under control and can be easily assimilated and utilized for the attacker's purposes.

It means that today,

a/ any commercial or other enterprise (system) is defenseless before the attackers who can access, transfer, modify, destroy the data, or otherwise intervene with the system's information flow

b/ if the system's assets and reserves are of any value for competitors or enemies, the system's owner might not achieve his operational and development purposes

c/ the cyber war, as well as any war that relies on the army and weapons, which are controlled through current cyber communication devices, cannot be won, especially, if the first attack disables the protective structures and takes control over the communications. With the currently employed methods and strategies of cyber defense and cyber attacks, it is possible to conclude that the attackers are fully capable of that.

Current Cyber Security Situation

At present, there is neither information network nor computer, which is invulnerable to cyber attacks. The attackers can access, control, modify, and assimilate any existing information network, computer, communication and controlling device; data within any existing network, computer, and communication device can be accessed, modified, transferred, and destroyed without permission or knowledge of the data creator/operator/owner.

The main problems include unidentifiable, uncontrollable, and unpreventable access, transfer, modification, and destruction of the data carried through the information nets, which compose the World Wide Web as well as other nets and subnets. All events, when such attacks have been identified, are the post–factum and mostly accidental discoveries. Although intrusion might be detected afterwards, it was not (and cannot be) prevented. Who was behind the attack, the attacker's purposes, and the scale of damage are not known; for instance, which data have been transferred, modified, destroyed, which internal or segregated networks have been accessed, which network already operates as the part of the attacker's domain, which network is in a process of assimilation by the attacker…

Details of the current cyber security situation:

1/ There is no possibility to prevent penetration, assimilation, and overtake of information nets, computers, and communication devices whoever the owner is – Department of Defense, Intelligence Service, research institution, financial, health, commercial enterprise, non–profit organization, or an ordinary citizen.

2/ There is no possibility to prevent remote cyber attacks, therefore, cyber espionage, access, transfer, modification, and destruction of the data whoever the attackers are – hostile or friendly governments, international criminal organizations, hackers, accidental intruders, disgruntled employees, competitors, spies of all types (industrial, commerce, political, research, etc.), curious persons, civil–liberties–watchers, politician–watchdogs, etc.

3/ There is no possibility to control own system(s) *{computer(s) and information net(s)},* communication and controlling devices *{telephones, GPS, etc.}*. The attacker can at any time and at the sole discretion, without owner knowledge (whoever the owner is)

— access the data

— monitor the system's activities

— read the files, which are currently evoked, processed, or stored by the system

— search the system's database

— initiate data transfer from the hard drive and any data storage, including attached removable disks, through data–processing hardware and peripherals

— turn on or off the system and its parts (e.g., webcam, microphone), especially those,

a/ which are constantly connected to the source of power

b/ which have installed batteries

c/ which can be connected to the source of power by remote control

— monitor the online session or real–time connection of the user (for instance, to remotely access desktop and "watch" the processed files after the user enters the bank secure portal to work with own banking account or while the user is engaged in other financial, commercial, and research activities).

4/ The system might be accessed, data might be transmitted, and the additional system's modifications might be done through satellites, wireless networks, radio, ground and mobile telephone cable devices and lines, broadband connections, and through other current means of data and energy transmission, access, and storage.

5/ If a newly purchased system or its components become the part of other information networks *{e.g., secret operational networks besides the Internet}*, the pre–installed and integrated malware might serve identification and ultimate disclosure and assimilation of entire nets.

In summary, there is neither a possibility to defend any system from cyber attacks with existing level of openness nor an ability to protect the most valuable assets, for instance, such as

a/ strategic, research, and financial data, information, and knowledge

b/ manufacturing and other systems operated and controlled through current information technologies.

Factors, Which Have Formed and Sustain the Current Cyber Security Situation

1. During many years, the systems were compromised and today they continue to be compromised by many ways, including

a/ worms, viruses and other kinds of malware planted through

— internet connections – emails, links, shared, opened, downloaded, and saved/stored files of all types, including doc., pdf., jpg., dll., exe., etc.

— web browsers

— legitimate software and applications (e.g., Adobe, Microsoft's Excel, Word, PowerPoint, etc., Google's applications, and the others) and pirated software and applications; both kinds of them might include hidden malware

— infected hosts, infected websites (especially social nets), and infected computers

— legitimate commercial IT services (especially, international outsourcing), during which the service providers are granted access to the system.

b/ Malware planted through peripherals, flash drives, data and music CDs (e.g., root–kit technology by Sony BMG), DVDs, and other devices used for data storage and transfer. Any of peripherals, which are initiated through installation of software or drives, and all devices, which by any means can be connected to the system and use its components, might

— contain hidden automatically self–installing software for modification of OS, periodical or one–time data access–transfer–modification–destruction–etc.

— install hidden directory

— initiate execution of arbitrary codes.

All of them can modify the system and transfer it under the attacker's control. In addition, infected peripherals and spare parts, which are used to repair the malfunctioning systems, also serve as the means of malware transfer.

c/ Malware planted through hardware and peripherals (hard drives, chips, modems, printers, keyboards, mice, webcams, microphones, authentication devices, and others) manufactured in China and other countries, which accommodate the organizations interested in access to the strategic, commercial, research, and other information that is in a possession of the US. These manufacturers (e.g., Lenovo, Sony) integrate the "malware" with the hardware or position it at the level (e.g., kernel, root–kit), at which the alien code cannot be identified by anti–virus or other protective software operating through Windows or other OS.

After activation of computer by its new owner, the integrated malware might

— initiate unidentifiable transmissions of the data masked under (or included into) the legitimate flow of information, for instance, such as initiated by the user transfer of data or pictures

— initiate modifications of the operation system and modification of the software installed at the computer

— initiate modifications of the interface, security and audit logs, so activities of the attackers would not be recorded and recognized by the owner's system, and the malicious services would remain "invisible" – undetectable

— connect the system with the site through which the attacker downloads files with malware

— initiate readiness for or execution of the commands transmitted through remote access feature

— include the system into the virtual domain, which is accessible, controlled, or maintained by the attacker

— include the system into the existing botnet

— assemble new malware from the unidentifiable by the host elements of the code transferred through emails, attachments, pdf, and any other types of files, etc.

d/ Legitimate and so–called "genuine" software, which is marketed as the means of protection, yet which contains the hidden codes that transfer the system under control of the attacker (e.g., anti–virus software by Kaspersky Lab).

e/ Malware installed by the manufacturers and owners of intellectual property to monitor activities of the users (e.g., copy–protection software by Sony).

f/ Software installed by the government monitoring structures for surveillance and with other purposes; the versions of such software stolen and modified by the attackers are not detectable by their own creators.

g/ Flaws and mistakes of design and configuration: operation systems, software, Web applications.

In summary, existing technologies allow not only creation of the present and future "points of entry" for the attackers; they

— make impossible identification of the "points of entry" prepared for and used by the attackers, at least until they are activated and until the owner of the system is able to identify them through the "abnormal" behavior of the system or through traces *{if any}* left by their activities

— provide possibilities to remotely activate or assemble the "points of entry" within the newly purchased system after its activation by the owner.

2. The recruited US citizens and the alien professionals (from any country, and especially, from China, Middle East, East Europe, and especially those with families and relatives in the mentioned countries, therefore, vulnerable to coercion) – spies, which are employed by the US manufacturers, security laboratories, government and intelligence structures,

— might transfer to their handlers the knowledge they access in the course of their employment in the US

— might plant the malware, modify employers' proprietary codes, operation systems, interfaces, and other parts of the systems – at any stage of software and hardware creation, manufacturing, and distribution.

If they have knowledge of the code, participate in software creation, or work in the security teams/departments/labs, they can modify any part of code and to prepare the "points of entry" or interfaces for the attackers. As the result, the manufactured in the US *{as well as abroad}* legitimate software, hardware, computers, peripherals, flash drives, and other parts of the systems might carry the codes, which would place the systems under the attacker's control at the moment of activation of the systems by new owners or at any other time adequate to the purposes of the attackers.

The possibilities to intervene with the processes of manufacturing of the system's components open additional possibilities for the attackers.

For instance, although the new computer or device was never (or is not) connected to the Internet, it might be activated remotely and transmit data to the attacker; a laptop might be turned on and data it carries might be transferred, modified, and destroyed without the owner's knowledge; hidden tracking device might transmit information concerning the current location and its change (in a case when the attacker needs physical – direct – access to the system through the infected device).

3. Any malware, which transfers the system under the attacker's control, is commonly spread through the upgrade and remote access features. After installation of malware, it modifies the system: the malware becomes the part of OS and as such, might not be completely removed without damage of the system or making it non–operational.

Also, advanced malware might contain auto–restore feature, which restores the components of malware identified and removed by the system's owner; it might also contain the self–modifying code, which would allow the further system's upgrades without removing the points of access for the attackers

4. The attacker can remotely reprogram, upgrade, and otherwise modify any system.

For instance, even if the owner disables or enables modem or any other hardware component, it might be turned on, enabled, or disabled. Besides, even if the system is powered off, the attacker can copy data from the hard drive and, in this case, without leaving any traces disclosing that files have been accessed.

5. The attackers have prepared the databases for access, transfer, and modification through legitimate database–creating, database–improving and data–mining software and applications, as well as through legitimate commercial *{that is registered and working openly as any commercial enterprise}* IT services.

Combined with the high degree of structuring of the World Wide Web (social, professional, financial, research, and other networks), the compiled and structured databases are ready to be harvested by *{or already are in possession of}* an attacker(s).

Situation Development

1/ Information grids. Use of information grid has three points of vulnerability:

a/ end user's terminal/computer/net – it might be already assimilated by the attacker who would have access to the data at the moment the data are created, transmitted, received by the data's owner

b/ middleware – the software, which makes possible existence of the grid and its operations, might be already modified by the attacker; it might contain the secret codes, which would facilitate control of the grid and open access to the data and the systems, which create–transmit–collect–store–process–modify–consume the data generated on and flowing through the grid

c/ center(s) controlling the grid – the controlling centers already might be assimilated by the attackers and work under the attackers' control.

The information grids are created with the purposes to facilitate and sustain scientific, research, and other operations, functioning of the state–country–society life–supporting systems (e.g., infrastructures, utilities, banks). Therefore, the access to them would provide the attacker with complete knowledge of the scientific, economical, and other potentials of the data owners. In other words, it would enable the attacker of complete control of the systems (access, assimilation, modification, destruction), which operate on the data flowing and generated on the information grids.

2/ Supercomputers. Whatever means of creation or transfer of the data are, the attacker's access to the end users' computers and nets makes entire systems vulnerable and data flowing through them unprotected and opened for the attackers. Besides, because of the previous access to IBM and European supercomputers granted to the researchers, these supercomputers might already receive the codes, which sustain illegitimate data traffic and enable the attacker of direct access to the data processing, modification, and transfer.

Moreover, if such relatively known and simple methods as phishing do work (as the recent events demonstrate), IT security is not capable to change the strategy of defense, even in dealing with supercomputers.

For instance, the published as "known" results of the recent cyber attack {*the first stage – phishing – was identified*} against the Energy Department's Oak Ridge National

Laboratory include access to the database of the research division. However, the possibility that the unidentified attacker(s) gained access to Jaguar itself or has activated the codes already planted within the attacked system (including “segregated networks”) might not be ruled out.

3/ Use of information nets, computers, communication devices. The planted or pre–installed “malicious” code might trigger malfunctioning of any systems controlled with or communicating through the infected devices: jets, power grids, medical and other devices, military installations, manufacturing plants, government agencies, and so on.

Current Methods of Defense against Cyber Attacks

1/ Patches. Operating systems and software manufactures work through “patches” and other modifications of the codes of existing operating systems and software.

These actions correct discovered defects or mistakes of the programmers and they close interfaces available for a specific malware. They do not prevent the attackers form discovering other “vulnerabilities,” or further modifications of the codes and interfaces. Although upgrade feature allows cleaning of the system from, for instance, unsophisticated worms tied to a particular version of the OS, it is not capable of disabling malware integrated with chip or hard drive or planted at the levels inaccessible by the operating systems.

Also, the upgraded OS still might contain interfaces accessible for the advanced software designed for the previous versions, or it might be accessed with the upgraded malware; therefore, the upgraded OS remain vulnerable.

Some advanced versions of malware might contain features of the evolving systems; such versions mirror changes of the upgraded OS and modify the elements of the code accordingly.

In addition, the more patches the less flexible current versions of OS become: there are limits of modification, which not influence the normal operations; behind those limits, the modifications, which for instance, restrict the flexibility, might have negative effect on performance, maintenance, and further upgrade of the existing OS.

2/ Anti–virus software. Efficiency of anti–virus software might be illustrated, for instance, with 2009 event when McAfee's anti–virus software blocked the OS files because it had read them as the virus, and thus, made impossible to boot PC. It means that anti–virus software might be incapable of discerning the OS files from the malware files, and "the fix" modifies the system without disabling the malware.

3/ Software/browser monitoring. For instance, InZero Secure PC, or two–computers–in–one, which includes the InZero Gateway module directly connected to the Internet with the secure environment in which, as the developers of InZero believe, virus cannot be executed. If the browser (or any other application) is not running or it has been changed, the module shuts down and clean copy is reloaded from the PC's read–only memory.

At first, the attackers can manipulate the boot code {*that it is possible when the system is powered off*}. The attacker might access RAM, to copy some or entire RAM contents, and then, after successful boot code modification, replace the "clean copy" of software with own "unclean" version; all these could be done unnoticeably for the owner.

Then, even the "secure environment" needs to be upgraded, if it is either intended to secure from new advanced versions of malware or to work with new advanced versions of the browser(s). Yet, upgrade might include malware or the code, which would modify, circumvent, or destroy defense capabilities of the system.

4/ Concept of the "borrowed hardware" –"Iron Clad" USB drive by Lockheed Martin Corporation. According to the creators, "Iron Clad" USB drive leaves no trace in the computer it was plugged in:

— it contains OS, software, settings, and files

— it can be used with any computer

— it contains own OS – OS runs off the flash drive

— the processed/generated/transmitted files do not touch the hard drive.

However, it means also that if "Iron Clad" borrows the hardware – monitor, keyboard, printer, and the others, it has to reach the user interface of the borrowed computer; otherwise, it would not be able to communicate with the borrowed computer (because of necessity to make the files accessible for the user).

If “Iron Clad” is connected to desktop or laptop, which have the user interface as the part of OS, the processed on the borrowed computer files will be, for instance, conveniently stored in the temporary files vault, therefore, can be recovered and accessed by other computer’s users. Possibilities of instant and unidentified access/transmitting data at the moment of connection of the Iron Clad and beginning of its operation also exist.

For instance, if “Iron Clad” is used on the controlled by the attacker computer, the data, which the user accesses with the borrowed computer peripherals, can be transferred to the attacker in the very moment of access by the user.

Then, if the borrowed computer is used for Internet access, it would inevitably leave “browser fingerprints”. Therefore, configuration of the computer, which is used by “Iron Clad,” might be identified, recognized, and monitored: the next appearance of the “Iron Clad” on another computer might be immediately recognized and the flash drive might be attacked through the borrowed hardware it uses, or other means.

As soon as the attackers, through remote access terminal, are able to monitor peripherals {*e.g., to “see” the screen, to transmit the printed file from the printer’s memory*}, they have access to all the files, which are processed on the borrowed computer. Even if the “Iron Clad” assumes full control of the peripherals, it does not change the borrowed computer’s boot.

Therefore, the “Iron Clad” might not be able to intervene with the borrowed system, if the borrowed system manages interface from the chip: all accessed through peripherals data as well as “Iron Clad” configuration can be stored at chip and consequently, retrieved or transmitted.

In addition, advanced malware might be already planted into the chip, which would transmit or to temporarily store – until the transmission – the processed files at the chip (instead of hard disk) at the very moment of access by the “Iron Clad” to the borrowed peripherals.

In addition, those who claim that the “Iron Clad” might be destroyed if stolen, do not take into consideration the technical capabilities of the thief–attacker. For instance, if device is stolen and it is not connected to internet, the “Iron Clad” creators can destroy it only

– either through radio or satellite transmission

– or planting the self–destruction code, which would be triggered, for instance, if the “Iron Clad” is not used some period of time, or if other terms/conditions of use take place.

Consequently, the destruction attempt might be unsuccessful, if the disassembly of "Iron Clad," access to the stored on it data, or its reverse engineering is made in the isolated center within walls impenetrable for the satellite– radio– other transmission, or in the time and under terms/condition compatible with pre–set terms/conditions known to the "Iron Clad" users.

5/ EADS Defense & Security "Security Cockpit" or "groundbreaking cyber security system." According to its creators, the described system is based on "Erudine's proprietary behavior capture" and discriminating technology, and it improves the ability "to respond to threats and attacks." It includes modules, which can "centralize" (to analyze and summarize) reports from all monitored systems and to react to attacks thorough "a central console."

Apparently, the solution is advanced techniques of monitoring of the system's traffic, bandwidth, log events, events correlation, calculation of metrics, security audits, access files, and other parameters, describing the system's behavior, and capturing new behavior added by the system's users.

The creators assume that

a/ they have an ability to identify the attacker through changes of the monitored system's behavior even if the user's behavior is changed, therefore, that they are able in real time to create new algorithms, which would describe the changing behavior of the legitimate users

b/ the "Security Cockpit" would serve secure real–time and high volume sensitive communications.

However,

— if the attack (as the access to the monitored networks) is recognized, again, it already happened, security breach has been done, and the data might have been read or transmitted; it is not prevention, it is the evidence of defeat

— the attack might be successfully hidden behind the high volume of real–time communications and the attacker's entry into the system (for instance, through the link within the transmitted rich contents file) might never be detected

— the monitored systems might be upgraded with the modified OS or software, which would provide access to the attackers as the part of systems' legitimate behavior, therefore, which would be accepted by "legacy evolution tool" as new behavior added by users

— the legitimate traffic might be rerouted by the end user, who receives the transmitted files, and the attacker might be masked under legitimate IP address

— for the purposes of the attacker, one–time transmission of the files might be sufficient.

In such a case, the hidden “sleeping” code might be activated within the monitored system(s) at the designated time, or after designated event. In addition, the legitimate inflow of data might contain the parts of the self–assembling code, which, in its parts, might not be detected by the monitors, yet, which, when complete within the system, would initiate instant and unstoppable transmission. In the best case scenario, such a transmission might be detected as the one–time unexplained traffic volume increase.

In general, the “Secure Cockpit” is as much secure as the systems it monitors are: even if it recognizes the attack and shuts down the system under attack, it is not able to prevent it. In a case when the attacker already accessed–transferred–modified–destroyed data or “a central console” identified the data transfer, the “Secure Cockpit” might not be effective.

6/ Open Source. The open source creators’ belief in security of the open source derivatives/products is based on the assumption that malicious code planting might be prevented through

a) open access to the code, which is open for mass participants, therefore, for plenty of code–auditors

b) constant development–changes of the OS *{which is in constant flux}*.

Such assumptions provide the false sense of security. For instance, they are not valid for the commercial fixed versions of the open source products, as well as they do not prevent “the instant strike” type of the attack, which initiates assembly and instant execution of the “malicious” code from the existing *{audited}* elements of the code.

The present relative “security” of the open source might be intentional tactic *{as it was the recent campaign propagating that Mac OS is worm/virus–invulnerable}*: after the government and intelligence structures complete implementation of the new open–source OS, the very accessibility and openness of the source code, as well as reverse engineering of application programming interface, would become the main issue.

Besides, modification of the OS is only one of many ways of the system’s assimilation. For instance, the attacker might avoid using OS, if the system already contains malware integrated with chip, or if data are copied while the system is powered off, or if data are transmitted through a network interface card, and so on

7/ Integration software with hardware, for instance, Chinese Kylin "secure operating system" combined with the "hardened chip" and improved remote access features.

Kylin, probably, is one of the versions, which might be developed on Security–Enhanced Linux (SELinux), a locked–down version of the operating system. According to the published information, in addition to "hardened" OS, Kylin sits on "a secure microprocessor that, unlike some US–made chips, is known to be hardened against external access by a hacker or automated malicious software."

However, there are publications concerning another direction of attacks on the systems: "hardware hacking," which would make Kylin vulnerable, therefore, unreliable in the same manner as other systems are.

8/ Encryption and password protection. In a case of transmitting the encrypted files – if the attacker has access either to a system–point of transmitting or to a system–point of receiving the data, the passwords, encryption keys, and other "protective" information might become the attacker's possession at the moment when the system becomes the part of attacker's botnet and controllers decrypt the data, or retrieve it from, for instance, Window Protected Storage for the encrypted information or from the browser.

WinZip and other encryption software used by government and other owners might also be deciphered by retrieving/reproducing the underlying algorithms.

In general, encryption is secure as much as the points of encrypting–deciphering–transmitting–acceptance of the information are secure.

9/ Finjan's Vital Security gateway (FVSg). Finjan's Vital Security gateway analyzes code on Web sites and blocks sites that it identifies as malicious.

This strategy is referred as the "step beyond the URL–based filtering approach"; it is described as "real–time content inspection technologies." According to Finjan's advertisements, FVSg is able to analyze the code embedded within web content or files, to identify even dynamic obfuscated code, to determine the results of its execution "in real time before it can reach end users," and to shut down the malicious web site. In order to provide such a service, Finjan inspects the contents, breaks the code into parts, and identifies the code's capabilities; then, if the code is identified as the malicious, it blocks its execution.

It means that to operate accordingly to advertised possibilities, Finjan needs

– either to have the database of existing malicious codes

– or to possess abilities to instantly execute the code and to determine the possible damage for the system.

Published information concerning Finjan's strategy leads to the inference that it might be effective only if FVSg

a/ identifies the code before it is admitted into the system

b/ after breaking the code into the parts, deciphers the code's capabilities

c/ prevents the code's entry into the system

d/ has special controlling system, which is separated from the monitored net(s) and is dedicated for trial execution of the code (so, trial execution of the malicious code would not accomplish the purposes of the attacker).

However, parts of the system do not provide the complete information of the capabilities of the system. It means, that the parts of the code might not reveal the actual code's potential, purposes, and results of its execution, for instance, as it might be in a case of transmission of the self–assembling code (which might be written with the same elements of the code as any legitimate software does). Besides, FVSg does not prevent data outflow–transfer initiated by the code already planted or assembled within the system, especially, if such a transfer is covered with the legitimate data traffic.

10/ NSA's classified software known as Einstein and Tutelage intended for internet traffic screening and monitoring with access to email and other transmissions through all channels of communication.

According to published information,

a/ Einstein is intended to become the early warning system concerning intrusions into monitored networks, near real–time identification of malicious activity, and automated disruption of the malicious activity

b/ after completion of the third phase, Einstein would possess the intrusion prevention capability, which will provide owners of the monitored by Einstein networks with "the ability to automatically detect and disrupt malicious activity before harm is done to critical networks and systems"

c/ NSA's database and hardware would be used to protect the networks of government agencies. The telecommunications companies will have to (or already do) route the Internet traffic through a monitoring box, which would search for and block computer codes designed to penetrate or otherwise compromise networks. If the monitored traffic contains the codes, which coincide with the database, the codes are blocked. In the same time, the quantity of access points has to be reduced.

Apparently, the NSA's method of defense is similar to Finjan's "unified web security solutions"; it might be based on inspection of the contents and comparison of the codes flowing through the internet traffic with the codes in the NSA's database of legitimate software codes and the NSA's database of the codes created by the hackers and used to attack and assimilate the existing nets.

The belief in effectiveness of this method of cyber protection might be founded on assumptions that Einstein with the monitoring box are sitting "on the traffic," without direct connections with the source and the recipient of the transmitted data. Consequently, it is assumed that

a/ neither hardware nor software can be compromised (modified or replaced by the malicious code) by the contents of the inspected flow of data

b/ as soon as there is no direct contact with the source and the recipient of the data flow, neither NSA's hardware nor NSA's software might be compromised.

Evidently, the ultimate efficiency of the Einstein (as well as any other software based on the same principles of operation) should be limited by

a/ collected database of malicious codes and other information concerning sources and purposes of the attackers

b/ abilities to distinguish between legitimate code intended to upgrade current systems and malicious code

c/ abilities to decipher the dynamic obfuscated code, or the code encrypted with other methods, which in addition to the usual script, might be hidden within the rich content files (e.g., pdf, flash), embedded into the apparently legitimate code, or communicated through contents of the transmitted files

d/ abilities to detect the parts of the self–assembling code and the points of access already existing within the monitored systems

e/ abilities to define and then, to detect "abnormalities" of the traffic and transmitted packets

f/ abilities to identify the source and destination IP addresses that in the case of malicious attack might be hidden or masqueraded under the legitimate nets

g/ technical parameters of the NSA's hardware.

For example, in a case of World Wide Web and 4GE LTE networks traffic monitoring {*for instance, there are about 4.5 billion wireless users; according to AT&T Wireless data – one 3G iPhone user generates data traffic equivalent 30 basic feature phone users*} and inspection of all types and transmissions of converged Evolved Packet Core packages for all types of traffic (data, video, voice circulating within all–IP core networks) would demand resources exceeding the capacities of existing world–wide computer grids, even if they are sustained by all known supercomputers. Besides, such employment of supercomputers would demand open and trustworthy cooperation of all countries that have supercomputers and access to the computer grids *{at the present stage of the international affairs, such cooperation does not seem to become the reality}*.

In the US, the unification of traffic and sustaining networks is accomplished through AT&T, which after merger with T–Mobile would control more than 97% of the US users. However, all–IP core networks are susceptible to all kinds of cyber attacks similarly to ordinary LAN, especially, classical DDoS attacks. It means that after entering into any of the networks – in the US or in other countries – controlled by AT&T, the malicious codes would spread over the entire net of nets.

For instance, if the US–wide AT&T network will be infected with malware intended for destruction of the US communications (e.g. similar to Stuxnet applied for destruction of the Iranian nuclear site and now resurfacing within different systems of the different states), the entire net controlled by AT&T can be cleaned only by replacement of the infected networks.

Concerning networks of other (not communication) companies: although NSA's Einstein might be effective for blocking the attacks at the lowest levels of complexity, it will not work in the following cases

— transmissions of the parts of unknown self–assembling codes, for instance, such as the pixel patterns in jpg files, or formatting specifications for the files created by Word or other applications, or within the rich contents files; for example, in a case when the system already is programmed to accommodate code's assembly and subsequent execution in a particular time, after a particular event, after database reaches particular parameters, or after/during communication with particular IP addresses or servers, Einstein will not be useful

— when the attacker transmits newly written codes (or the parts of self–assembling codes) unknown to NSA

— when the systems, which are the parts of the botnet, are used to execute code–disassembly before entering the NSA's traffic monitoring box and code–reassembly after exit the NSA's traffic monitoring box

— when the systems, which are the parts of the botnet, are employed as the carriers of the parts of the code; in such a case, they might execute the attack when all of them are operational and at the designated time, which NSA would detect only after completion of the attack.

— internally initiated transmission of data (from the monitored government nets), which might not contain the code or even parts of it, yet, simply transfer the data (for instance, stored social security numbers of some personnel) to the attacker masked under legitimate IP address or the attacker who controls the legitimate IP address

— already compromised systems, which contain the "sleeping" codes intended to transmit, modify, or destroy the data in the time convenient for the attacker's purposes or after specified event (for instance, after beginning of the manufacturing processes or other actions).

Besides, with the current growth of traffic of data, software, and applications, NSA's Einstein or any program based on contents inspection and comparison of the legitimate codes (or any other data) with the codes (or any other data) flowing through the internet, might be successful only if it uses supercomputers or computing grids capable to perform astronomical quantity of transactions required for traffic contents control. However, it might not be uncompromised supercomputers and grids already.

It means that, if Einstein is run on the compromised computer–part of the grid or on the compromised supercomputer, the attacker might gain access to the Einstein's code, therefore, modify or circumvent it.

In addition, it might be a problem with detection of "malicious" code. "Maliciousness" of the code is defined by the incompatibility with the operations for which the system exists, and the results of the code's execution. For instance, code might be defined as malicious in a case when it

– either enables unauthorized by the owner access, transmission, and modification/destruction of the data

– or otherwise intervenes with the purposes of the system's owner.

It means that Einstein should be constantly upgraded to be able to determine new "malicious" codes, and that improved data–mining features must be added constantly. Consequently, those who run Einstein must be able to recognize maliciousness of the code as incompatibility with the system purposes. It means that they have

– either to ascend at the levels of owners of all systems they attempt to protect

– or to assimilate all systems.

In summary, it is evident that the Einstein's creators assume that Einstein might achieve such level of efficiency that it would monitor, decipher, censor, own, and operate the entire content of the US and world traffic and block

— unknown or defined as "malicious" codes from entry into the monitored systems

— unauthorized transfers of the data from the monitored systems.

In addition, Einstein is software, and as any software it might be modified even without knowledge of those who created and who employ it for the systems protection.

11/ Clouds. In general, the basis of this method of data operations is the concept of dumb terminal. Although cloud method of data handling might decrease the access to the points of data creators and operators, it would not prevent the unauthorized access to the data stored "on cloud."

Besides, the cloud servers and data service providers' nets are vulnerable to all kinds of malware and cyber attacks as the ordinary nets are.

Additional difficulties for the data creators–users–owners would include loss of access to their own data and the data's permanent loss in a case of crush *{as it happened, for instance, with some Federal government and business sites when Amazon's EC2 in Northern Virginia crashed in April, 2011}*.

12/ Thales' CYBELS (cyber expertise for leading security) solution. According to Thales' publication, CYBELS solution, which was launched in 2010, is "an open–ended and modular system integrating security tools into a security centre dedicated to active cyberdefence."

Thales sees passive defense systems and protocols, such as firewalls and isolation, as no longer adequate protection against increasingly sophisticated means of cyber attacks.

CYBELS is hypervision system that according to Thales, offers a global picture of information systems security, merging and processing information from different sources. The results include dynamic risk–processing, the ability to assess the impacts of a cyber attack, and guidance how to respond (by suggesting appropriate actions).

According to Thales, "swift detection of any attack is the first task of the cybersecurity solution, which is performed automatically. The attack is also rapidly analyzed, so that operators in a permanently staffed cybersecurity center can respond accordingly."

This system is offered to the Middle East market, and it leaves the buyers with the same vulnerabilities and problems, which all other systems in other regions of the world have.

The Thales' solution illustrates the mainstream of the defense methods and strategies: it is improvement and acceleration of the risk–detecting techniques and response on the detected attack. CYBEL is the system built in the same conceptual foundation that the EADS Defense & Security "Security Cockpit" (see 5/ above), or even a simplified version of the "Security Cockpit."

CYBEL is also inadequate solution, because it does not decide the main problem – how to prevent intrusion, the unauthorized access into the system – the cyber attack itself.

Conclusion

From the philosophical point of view, it might be concluded that

1/ the current meaning of the "absolute power" is inseparable from

a/ the hidden access to and control of the information resources and computing/communicating devices, which belong to the enemies, opponents, and owners of the valuable resources

b/ abilities to protect own information resources (nets, data, transfer and use of information) from unauthorized access, transfer, modification, and use

2/ current owners of the information networks do not possess such power.

From the practical point of view, it might be concluded that the current methods of cyber defense are not effective: they leave those who rely on them exposed to the unpreventable and, in many cases undetectable even after exposure, attacks.

Then,

A.

— If to consider speed of expansion of botnets, level of sophistication of the malware and arbitrary codes, methods of assimilation of existing systems

— If to analyze information concerning cyber vulnerability and inability to protect existing systems (e.g., reports concerning cyber attacks, strategies of defense, attempts to prevent intrusion, analyses of strategies applied by hackers, botnets herders, criminal circles praying on Internet users, and existing methods of detection and defense)

— If to take into consideration the factors listed above,

— If to analyze the current methods of cyber defense,

it might be concluded {***1** through **5***}:

1/ Currently, there is no effective method of defense, which would secure existing systems from cyber attacks and which would prevent consequent assimilation of the systems by the attackers.

2/ All systems are open to unidentifiable and uncontrollable access, transfer, modification, and destruction of the data through all stages of existence: manufacturing, installation of software, modifications, sale, technical support, functioning, upgrade, receiving and transfer of data, and so on.

None of existing operating systems (including Windows, Linux, Mac OS, UNIX, and the Open Source derivatives) is capable of preventing penetration, installation, and execution of viruses, worms, and any malware and at any level of the information net, computer, and other device.

Any system *{including research, financial, and other networks}*, irrespective of its connections/non–connections to the World Wide Web,

— either already is under the attacker's control

— or will come under control of the attacker in the nearest future.

Currently, no one system might be considered as uncompromised and safe if

— it is accessible through the existing nets

— it is employed to create, store, and process files transmitted or received through the information networks, removable hard and flash drives, cds, and other memory storage devices

— it operates on Windows, Linux, Unix, Mac OS, Open Source derivatives, or any of other current operation systems

— it is assembled with the components manufactured abroad or in the domestic facilities accessible for the foreign intelligence penetration

— it includes modems or other receiving–transmitting devices, therefore, if it is capable of

a/ operating through the wireless, broadband, and other networks and lines of transmission of data and energy

b/ receiving radio and satellite transmissions

3/ All systems are open to access, modification, and remote control by the attackers. The control of systems connected to the networks composing World Wide Web belongs not to the owners; the control of such systems belongs to anyone who has access to the Web and who possesses the technical skills sufficient to access and to manipulate the systems, their components, and their connections.

Some systems already are not run by their owners, although the owners still have the systems in their physical possession and are allowed to conduct business and routine operations.

4/ The World Wide Web has been transformed into the assembly of the layered structures–nets, which, in addition to the Internet and legitimate secured nets and subnets, includes different combinations of the systems controlled by different groups, criminal organizations, companies, and individuals. The structural components of the WWW undergo unification and are in a constant process of temporal or constant concentration around the “cores”–centers, which are run by the different kinds of attackers.

5/ Apparently,

a/ the war for the control of the entire World Wide Web advanced into the second phase

b/ those who are behind the attackers already began the manifest modification of the World Wide Web according to their purposes.

{In general, any conquest includes the following stages:

— the first stage: 1 – preparation, 2 – attack, 3 – coming into possession or inclusion into own domain

— the second stage: 4 – assimilation; this stage includes modification of the behavior of the conquered according to the purposes of the conqueror, e.g., establishment and implementation of new rules of behavior for the conquered; 5 – preparation for utilization and consuming of resources of the assimilated, and so on.}

For instance,

— when major search engines deliver search results, in the top of page, they list websites that spread malware or contain links to the systems assimilating the visitors' computers

— so–called "business intelligence software" (currently, "database improving" software) offers improvement of identification and classification (e.g., through tags) of information; the actual purpose might be facilitation of exploration and harvesting (extraction) of the information stored in the systems, because for the successful harvesting, it is necessary to separate the valuable information from the information identified as the routine, maintenance, and noise. Combination of development of the search engines and data–mining applications with business intelligence software acquired by the data owners facilitates data–extracting for the attackers

— IT services during which the service providers are granted access to the database; for instance, such as remote back up, remote processing and storage

— world–wide scales of the attacks.

Such coordinated efforts provide a glimpse of the scales of the existing control.

B.

All existing methods of defense – conventional virus/malware–protection software, signature–based intrusion detection techniques, software and browser's code analysis, web and traffic contents analysis, monitoring of the system's bandwidth and other parameters, system's user behavior monitoring, read–only software, hard–drive encryption, password protection, "strengthening OS" and "hardening software" *{e.g., integration of chip and software}* – are the attempts to detect the attack.

All of them are responses or, in more advanced systems, attempts of prevention the attack by restricting or even interruption of traffic (e.g., "kill–switch" for shutting down the nets in a case of massive cyber attack, for instance, such as an attack intended to disable or destroy utilities grids and other vital systems), censoring the information contents, or restricting flexibility of the operations. Consequently, they are not effective.

C.

The current strategies of defense include

— monitoring, inspection, and evaluation of the internet traffic and its contents

— inspection of the websites, their script, contents, and connections

— technical modifications of hardware and integration of hardware with software with the attempts to decrease possibilities of remote modification and remote control of the systems.

Ultimately, such strategies might

a/ restrict operational flexibility of the systems developed for centralized (remote) upgrade, maintenance, and control by the software and hardware manufacturers

b/ destroy foundation for the current IT services such as remote back up, remote storage and data processing, cloud application platforms, and other

— code deciphering, identification and verification

— identification of the source of transmission

— restrictions of flexibility of existing systems with the purpose to prevent their modification by the malicious codes.

The conceptual foundation of the current strategies includes assumptions of the abilities to defend the systems through

— control of the flow and contents of data initiated by the sources, which are uncontrollable and unidentifiable in the real–time – the moment of attack

— the capacity to restrict flexibility of the systems created to be flexible, modifiable, and adjustable in accordance with the parameters of the flow of the data – – the World Wide Web traffic.

As soon as such assumptions contradict the nature of the World Wide Web created for the free and unrestricted transmission and modification of the flow of data, any strategy of defense based on these assumptions cannot be successful.

The most advanced methods of the defense, which might be developed on the same conceptual foundation, are deciphering and identification of the malicious code and mock execution of the identified code, so the results of its execution by the systems might be predicted.

However, if to realize that the "maliciousness" of the code *{the "malicious" code is the code, which is inconsistent with the website official purposes, or which initiates activities identified as attack}* is defined only by the results of its execution for the legitimate owners and users of the systems (hardware, software, peripherals, connections, etc.) and the data produced and transmitted by the systems, it becomes understandable that in fact, there is no chance of absolute protection developed on existing concept of data creation, storage, and transmission.

In summary, all current methods of cyber defense are based on the classical strategy of failure: ***response***, and only if and after the attacker is identified. If the attacked system is not able to identify the attacker, it unnoticeably might come under control and can be easily assimilated by the attacker and utilized for the attacker's purposes.

It also means that today, the cyber war, as well as any war that relies on the army and weapons operating and controlled through cyber communication devices, cannot be won, especially, if the first attack disables the protective structures. With the currently employed methods and strategies of cyber defense and cyber attacks, it is possible to conclude that the attackers are fully capable of that.