Trust in Cyberspace: New Information Security Paradigm

R. Uzal, D. Riesco, G. Montejano
Universidad Nacional de San Luis
San Luis, Argentina
ruzal@uolsinectis.com.ar
{driesco, gmonte}@unsl.edu.ar

N. Debnath
Department of Computer Science
Winona State University
USA
ndebnath@winona.edu

Abstract*—This paper is about the differences between traditional and new Information Security paradigms, the conceptual difference between "known computer viruses" and sophisticated Cyber Weapons, the existence of a Cyber Weapons "black market", the differences between Cyber War, Cyber Terrorism and Cyber Crime, the new Information Security paradigm characteristics and the author's conclusion about the new Information Security paradigm to be faced. Authors remark that recently discovered Cyber Weapons can be easily described as one of the most complex IT threats ever discovered. They are big and incredibly sophisticated. They pretty much redefine the notion of Information Security. Considering the existence of a sort of Cyber Weapon black market, very sophisticated malware in terrorist and criminal hands changes the Information Security scenario and changes also the Information Security paradigm. Obtaining people's trust in cyberspace is a new challenge which implies working on the improvement and reinforcement of information and communication security. Paper points it must be established that, Information System specifications must have a new balance between functional and non-functional specifications. Currently, and in actual terms, functional specifications have priority over the non-functional ones. Project budget and other resources must be allocated to obtain goals related to concepts like Confidentiality, Integrity, Availability and Authenticity in the context of non-functional specifications. In the new Information Security paradigm, Security must be the key issue in an Information System conceptual design, development, implantation, use and maintenance.

***Keywords-** Information Security paradigm change; Cyber Weapons; non-functional specifications*

I. INTRODUCTION

Insecurity is an intellectual perception, accepted by an individual or a society as a clear example, model, or pattern of how things work in the Cyberspace. Not all software and information operate the way people expect. Several recent examples have proven that cyber attacks may cause physical damage to premises, showing the need to reinforce security in data transmission channels. Therefore, a new paradigm for managing the information security arises from the intention of obtaining people's trust in cyberspace. Definition of "paradigm" was used first by the US science fiction writer Thomas Kuhn [1] to refer to theoretical frameworks within which all scientific thinking and practices operate [2].

It is known that, in several nation-states, Cyber War units from other "friendly nation-states", are placing a trapdoor in civilian networks, planting logic bombs in electric power grids and infrastructure for destruction [3]. It is evident we are facing new and very important changes in the traditional Information Security paradigm. Paradigm shift means a fundamental change in an individual's or a society's view of how things work in the cyberspace. For example, the shift from the geocentric to the heliocentric paradigm, from "humors" to microbes as causes of disease, from heart to brain as the center of thinking and feeling [4]. Criminal hackers could detect some of those placed "military logic bombs" and use them for criminal purposes. This is not a theory. It is just a component of current and actual Information Security new scenarios.

This presentation is about the differences between traditional and new Information Security paradigms, the conceptual difference between "known computer viruses" and sophisticated Cyber Weapons, the existence of a Cyber Weapons "black market", the differences between Cyber War, Cyber Terrorism and Cyber Crime, the new Information Security paradigm characteristics and the author's conclusion about the new Information Security paradigm to be faced.

In this paper, authors point to top Cyber War and IT expert's opinions and trustworthy sources in order to obtain conclusions using the synergic effect of those expert's opinions.

II. "TRADITIONAL" INFORMATION SECURITY PARADIGM

"The Internet's crucial role in modern life, commerce, and government underscores the need to study the security of the protocols and infrastructure that comprise it. For years, we've focused on endpoint security and ignored infrastructure weaknesses. Recent discoveries and initiatives highlight a simple fact: the core is just as vulnerable as the edge" [5]. Facing those infrastructure weaknesses and overcoming them, is a key issue in the context of the new Information Security paradigm.

Traditionally it was generally admitted that Information Security Concepts are important in creating security policies, procedures, and IT business decisions. This work examines the effective applicability of traditional Information Security just understood as Confidentiality + Integrity + Availability + Authenticity. As an example, the paper contents show the importance of Legal, Political and Human Resources Management issues in the new Information Security paradigm.

Nowadays the threats to Information Security have grown dramatically in scope and complexity. Sophisticated

Published by Atlantis Press, Paris, France.

Cyber Weapons and Cyber War strategies presence and their actual impact in corporations and other organizations environment, have changed the “game rules” in the field of Information Security. This paper shows the true state of government, corporations and organizations in general terms security environment, challenges and readiness and we also are presenting an outline of a needed new Information Security paradigm.

In advance we can mention that, mainly for Defense officials, Cyberspace have become a new Operational Domain [6] [7] as the traditional air-sea-land. Now, in actual terms, Cyberspace includes virtually every use of a computer, including those built into weapons, vehicles, decision support tools, and everyday life. Currently most of military missions, in some sense, occur in cyberspace. As examples we can mention combat, including counter-insurgency; military support to national priorities (counter - drug, border security, etc.); disaster relief and humanitarian assistance and conflicts between nation states in the Cyberspace [6][7][8][9][10].

III. From Computer Virus to Cyber Weapons

“A computer virus described as a Cyber Weapon, the most complex ever created has been discovered in thousands of computers in the Middle East” [8]. It is kwon that this new kind of computer virus, called Flame, discovered by security experts Kaspersky Labs, marks a new era in Cyber Warfare [10].

Flame (approximate size of 20 megabytes) is the third major Cyber Weapon detected / identified after Stuxnet (approximate size of 2 megabytes), the worm that attacked Iran's uranium enrichment plant at Natanz in 2010, and Duqu, a data-stealing military-oriented malware.

Flame computing algorithms complexity is over a hundred times the “usual” complexity of “standard/traditional” PC viruses. Flame is designed, primarily, as a spy; basic functions include stealing information, for example the contact list of mobile phones close to infected computers, turning on microphones and web cams also on infected PCs to listen to conversations and to recognize persons. Flame acts also as a sort of “software bus” allocating different Cyber Weapons / Computer Viruses in its “software slot” according to the nature of different missions it must face. Flame complexity shows that, in its creation, the resources of one or several nation-state have been required. Flame is the most complex piece of malicious software discovered to date, said Kaspersky Lab senior researcher Roel Schouwenberg [11][12], whose company discovered the virus acting according to United Nations orientation. It is suspected that Flame was “working” undiscovered for five years. Paper author agree with Schouwenberg: “The only logical conclusion is that there are other operations ongoing that we don't know about”.

Information Security must be now mainly focused on new weapons and types of attacks we can describe using, as a reference, Stuxnet Cyber Weapon. Many security experts, including U.S. officials, have said that it was likely that Stuxnet was made by the U.S. with Israel assistance [9]. The Stuxnet worm scheme consists of the following modules: structural module, payload module, propulsion module, guide module and communication module. This scheme looks like a missile conceptual architecture, as it is analogous to a missile conceptual design. Stuxnet could not be compared with “traditional” computers virus or known worms and trojans. Stuxnet is also a sophisticated example of programming multi-paradigm: Imperative – Algorithmic paradigm; Object Oriented paradigm and Functional paradigm. The Stuxnet-like Cyber Weapons development era implies an important effort and knowledge level on information security.

Stuxnet is a reference of the new Information Security paradigm needed. Stuxnet is not the work of a small group of hackers, as when its structure and algorithmic complexity is analyzed, it evidences several years of a high level skilled programming team, and very high development costs.

IV. Cyber Weapons: From Cyber War to Cyber Terrorism and Cyber Crime

1) According to The Guadian, Spiegel and others [11][12] a three week wave of massive Cyber-Attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with NATO urgently examining the offensive and its implications. While Russia and Estonia are embroiled in their worst dispute since the collapse of the Soviet Union, a row that erupted at the end of last month over the Estonians' removal of the Bronze Soldier Soviet war memorial in central Tallinn, the country has been subjected to a barrage of Cyber Warfare, disabling the websites of government ministries, political parties, newspapers, banks, and companies. NATO has dispatched some of its top experts to Tallinn to investigate and to help the Estonians beef up their cyber defenses. "This is an operational security issue, something we're taking very seriously," said an official at NATO headquarters in Brussels.

2) Richard Clarke reported [6]: “Syria had spent billions of dollars on air defense systems. That 2007 September night, Syrian military personnel were closely watching their radars. The skies over Syria seemed safe and largely empty as midnight rolled around. In fact, however, formations of Israel Eagles and Falcons had penetrated Syrian airspace through Turkey. Those aircraft designed and first built in the 1970’s, were far from stealthy. Their steel and titanium airframes, their sharp edges and corners, the bombs and missiles hanging on their wings, should have lit up the Syrian radars like the Christmas tree illuminating New York’s Rockefeller Plaza in December. But, they didn’t. What the Syrians slowly, reluctantly, and painfully concluded the next morning was that Israel had “owned”, using a Cyber Weapon, Syrian air defense network the night before. The Syrian ground based controllers had seen no targets. This is how war would be fought in the information age, this was Cyber War”.

3) USA Today announced, July 9, 2009 [13], that “U.S. authorities say they are eyeing North Korea as the origin of the Cyber Attack that overwhelmed government websites in the United States and South Korea. Targets of the most widespread cyber offensive of recent years also included the

National Security Agency, Homeland Security Department and State Department, the NASDAQ stock market and The Washington Post, according to an early analysis of the malicious software used in the attacks.

4) Tony Capaccio and Jeff Bliss [14] report that "Computer hackers, possibly from the Chinese military, interfered with two U.S. government satellites four times in 2007 and 2008 through a ground station in Norway, according to a congressional commission. The intrusions on the satellites, used for earth climate and terrain observation, underscore the potential danger posed by hackers.

5) David E. Sanger and Eric Schmitt [9] reported "The top American military official responsible for defending the United States against Cyber Attacks said Thursday that there had been an important increment in computer attacks on American infrastructure between 2009 and 2011, initiated by criminal gangs, hackers and other nations.

6) The Wall Street Journal [15] reported in April that Russian and Chinese spies had penetrated the U.S. electric grid. Lawmakers are pushing at least three different proposals to boost Cyber Security in the electric sector, including measures that would give the federal government authority to issue regulations to combat imminent threats. President Obama on June 15, 2011, had admitted "Cyber intruders have proven our electrical grids".

7) Iftikhar Alam [16] from "The Nation" (Pakistan) on December 05, 2010 reported that The Friday nights Cyber Attack on the website of Central Bureau of Investigation (CBI) - the top civilian investigation agency of India - in response to the attack on 40 Pakistani websites has intensified the cyber war between India and Pakistan which had started in 1998. According to the IT experts, there are hundreds of highly professional hackers operating in both the countries.

Could the Cyber Weapons used in the aforementioned examples be transferred from military environment to criminal hands? This question and its answer are closely related to the Information Security paradigm change introduced in this presentation.

V. A Cyber Weapons "black market"?

1) David E. Sanger [17], just released his new book "Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power". It an excerpt from the book, Sanger claims current U.S. President, Barrack Obama, has been involved in a secret Cyber War with Iran, for his entire Presidential term. Sanger reports that Obama has ramped up a Cyber Weapons operation originally started in the Bush regime, codenamed "Olympic Games". The "Olympic Games" Cyber Attacks were aimed against Iran's nuclear enrichment facility. The specific Cyber Weapon aimed at Iran's nuclear enrichment facility has been dubbed Stuxnet. Stuxnet is a virus that's purpose is to sabotage the centrifuges for creating weapons-grade enriched uranium. It was used against Iran in 2010. The reports about this new Stuxnet virus comes out just a few days after the UN has warned the Middle East about a virus, called the Flame virus that is now on the loose. Sanger's sources say that these cyber weapons are being created and used in joint by the US, and Israel. However, as is the nature of covert warfare, these allegations have been completely denied by US and Israeli officials. The Obama regime has recently admitted to using Cyber Weapons, but only in use against Al Qaeda terrorists. They have not admitted to using Cyber Weapons against the Iran government yet. Iran has found computers in their facilities that contain the Stuxnet and Flame viruses. The Flame virus is now on the loose and could be in anyone's hands. These Cyber Weapons could easily be sold on the black-market to cyber-terrorists. Now that the US/Israel's enemies have these Cyber Weapons in their hands, it's only a matter of time before the coding of these viruses is reverse-engineered and used against us".

2) Sam Kiley [18], is a the Defense and Security Editor of Sky News, a 24 hour television news service operated by Sky Television, part of British Sky Broadcasting. He is an award-winning journalist of over twenty years' experience, based at different times of his career in London, Los Angeles, Nairobi, Johannesburg and Jerusalem. According to Sam Kiley, Stuxnet, the Cyber Weapon that was used to disrupt Iran's nuclear program has been traded on the black market and could be used by terrorists.

VI. Cyber War, Cyber Terrorism and Cyber Crime consequence: The Information Security paradigm change

United States government security expert, Richard A. Clarke, in his book Cyber War [6], defines "Cyber Warfare" as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".

In this sense, The Economist describes cyberspace as "the fifth domain of Warfare,"[19] and William J. Lynn [20], U.S. Deputy Secretary of Defense, states that "as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in Warfare . . . [which] has become just as critical to military operations as land, sea, air, and space."

In parallel, the FBI [21][22] defines terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. Cyber Terrorism could thus be defined as the use of computing resources to intimidate or coerce others. An example of Cyber Terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge. It sounds theatrical, but these things can and do happen. "Cyber Terrorism is a component of Information Warfare, but Information Warfare is not Cyber Terrorism.

Also the Federal Bureau of Investigations (FBI) recognizes four instances of Cyber Crime [21][22] a) Cyber Crimes against children (usually involving child pornography or child rape), b) Theft of intellectual property, c) Publication and intentional dissemination of malware, d) National and international Internet fraud.

Now we know that it is possible that sophisticated Cyber Weapons used in conflicts between nation-states can be traded in the black market and could be used by terrorists or criminals. It is not a theoretical speculation; it is a real world situation. Recently, the authors of this research met the engineer in charge of an effluent plant belonging to an important industrial complex in South America, who reported that a "Stuxnet like" malware took the effluent plant control and changed the operation parameters causing polluting materials to be dumped, even when thr effluent plant monitoring panel displayed that everything was in normal operation conditions.

VII. New Information Security paradigm environment

Taking into account the new scenarios description, Information Security needs an important paradigm shift in order to successfully protect information assets. Organizations must effectively change from an Information-System-focused Information Security management to an Organizational-focused Information Security management, requiring a well-established Information Security Management System (ISMS) [23]. Current accepted concept of ISMS must be improved and optimized regardless of the fact that this improvement and optimization requires higher risks, investment, knowledge and skills. This improved and optimized ISMS must address all aspects in an organization that deals with creating and maintaining a secure information environment using a multidisciplinary and interdisciplinary approach. It also requires an intelligent mixture of aspects such as clear policies, a very intelligent use of standards, effective guidelines, technology support, legal support, political support and a very specialized human resources management.

In this context, the two Koreas provide a very interesting paradigms contrast to be studied. South Korea has high-speed Internet access reaching ninety five percent of its citizenry. This is the highest rate of access to the internet of any nation today. With this national emphasis on connectivity, South Koreans typically store their medical, banking and online shopping records digitally. This makes those networks more vulnerable to attacks as there are personal assets associated with those networks.

By contrast, North Korea has very little Internet connectivity, and is therefore not as vulnerable to external online attacks. Who would attack North Korea's Internet? By strongly restricting who has access to the Internet, North Korea can focus its limited resources on a few universities that may be the launching point for the recent Cyber Attacks, currently focused on their neighbor and rival South Korea, but which someday could be used on countries in the West. Generically, these are called asymmetric threats.

Obtaining people's trust in cyberspace is a new challenge which implies working on the improvement and reinforcement of information and communication security.

VIII. Conclusions

1) Recently discovered Cyber Weapons can be easily described as one of the most complex IT threats ever discovered. They are big and incredibly sophisticated. They pretty much redefine the notion of Information Security.

2) Considering the existence of a sort of Cyber Weapon black market, very sophisticated malware in terrorist and criminal hands changes the Information Security scenario and changes also the Information Security paradigm.

3) When a developed country government decided, for example, to bomb the nuclear installations belonging to a developing country or a terrorists training area, that developing country may not be able to respond using conventional military forces and / or conventional weapons. It may respond, developing Cyber War capabilities, destroying, for example, and important part of the international financial system in witch, that country has very little share. There are evidences that this kind of Cyber Weapons can easily be transferred from government area to criminal and terrorist groups.

4) The "use" of "Flame like" and/or "Stuxnet like" Worms / Trojans, in the context of dirty competition between huge corporations, could possibly start (if not already has).

5) Cyber Warfare is seen as a technology problem by technologists, a policy problem by politicians, and a profit problem by businesses. This confluence of concerns is likely due to the prevaling nature of technology in our daily lives. Additionally the confluence of concerns implies a multidisciplinary approach need in the context of a new Information Security paradigm.

6) The most effective protection against "Cyber Warfare like" attacks is securing information and networks. Important investment in security should be applied to all systems, including those "not critical", because any vulnerable system can be co-opted and used to carry out attacks. Measures to mitigate the potential damage of a "Cyber War like" attack include comprehensive disaster recovery planning that includes provisions for extended devastations.

7) At the level of nation-states, Cyber Defense units and at its related agencies, most intelligent best skilled Human Resources must be developing plans and capabilities to achieve "dominance in Cyberspace" to maintain the nation-state in the condition of a safety environment for government institutions, corporations and all kind of organizations.

8) In the short-term the defense agenda must include the implantation of a sort of "defensive triad": a) Capability of stopping sophisticated malware on the Internet at the backbone of Internet Service Providers level; b) prioritizing and strengthening the controls of the electric grid; c) increasing the security of the Defense area networks including the IT support for the top level decision making process.

9) It must be established that, Information System specifications must have a new balance between functional and non-functional specifications. Currently, and in actual terms, functional specifications have priority over the non-functional ones. Project budget and other resources must be allocated to obtain goals related to concepts like Confidentiality, Integrity, Availability and Authenticity in the context of non-functional specifications. In the new Information Security paradigm, Security must be the key

issue in an Information System conceptual design, development, implantation, use and maintenance.

REFERENCES

[1] Kuhn, Thomas, “The Structure of Scientific Revolution”, University of Chicago Press, 1962

[2] Business Dictionary http://www.businessdictionary.com/definition/paradigm.html

[3] Clarke, Richard A. and Robert K. Knake, Ecco, Cyber War, 2010

[4] Business Dictionary http://www.businessdictionary.com/definition/paradigm-shift.html

[5] Jose Nazario , John Kristoff , “Internet Infrastructure Security”, Published by the IEEE Computer Society, (Vol. 10, No. 4) pp. 24-25, IEEE, July/August 2012

[6] "Cyberwar: War in the Fifth Domain" Economist, 1 July 2010

[7] Lynn, William J. III. "Defending a New Domain: The Pentagon's Cyber Strategy", Foreign Affairs, Sept/Oct. 2010, pp. 97–108

[8] Rob Waugh, http://www.dailymail.co.uk/sciencetech/article-2151199/A-new-era-cyber-warfare-Virus-weapon-lurked-inside-thousands-computers-Middle-East-years.html Daily Mail, published 16:38 GMT, 28 May 2012

[9] David E. Sanger and Eric Schmitt, “New York Times”, July 26, 2012

[10] http://www.telegraph.co.uk/news/worldnews/middleeast/iran/9295938/Flame-worlds-most-complex-computer-virus-exposed.html

[11] Ian Traynor in Brussels, The Guardian, Thursday 17 May 2007, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia

[12] http://www.spiegel.de/international/world/old-wars-and-new-estonians-accuse-kremlin-of-cyberwarfare-a-483394.html

[13] http://www.usatoday.com/news/washington/2009-07-08-hacking-washington-nkorea_N.htm

[14] Tony Capaccio and Jeff Bliss, “Business Week”, October 27, 2011, http://www.dailymail.co.uk/sciencetech/article-2151199/A-new-era-cyber-warfare-Virus-weapon-lurked-inside-thousands-computers-Middle-East-years.html

[15] http://online.wsj.com/article/SB124528065956425189.html

[16] http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/politics/05-Dec-2010/PakistanIndia-cyber-war-begins

[17] David E. Sanger Confront and Conceal, Publisher: Crown (June 5, 2012)

[18] http://news.sky.com/story/820902/super-virus-a-target-for-cyber-terrorists

[19] "Cyberwar: War in the Fifth Domain" Economist, 1 July 2010

[20] Karen Parrish, Lynn: “Cyber Strategy’s Thrust is Defensive”, American Forces News Service, July 14, 2011

[21] http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror

[22] Federal Bureau of Investigations. “Cyber Investigations” http://www.fbi.gov/about-us/investigate/cyber/cyber

[23] http://www.itgovernance.co.uk/iso27001.aspx

Published by Atlantis Press, Paris, France.