World Risk Society

The Risk of Interconnected Computing

Álvaro M. Ferro

Abstract

This essay looks at interconnected computers as a risk origin to the society and as a source of menace to the survival of humanity. The author will try to create the basis for a discussion around the possibility of uncontrollable, de-localized and un-calculable risk from the use of interconnected computers. The main argument is that humanity is too exposed to humans own doing and that we can cause doom to ourselves by chance or intention through interconnected computers, and its defects. To do this, the essay will present the view of the author, according to whom the arguments can be pulled to two extremes: On one side the "*there is nothing new*" and on the other side the catastrophist view of "*the unknown unknowns*". In conclusion, it will try to sort out if the kind of threats from interconnected computers can be put side by side with pollution, diseases and war in a world risk society.

> *"In place of the old wants, satisfied by the production of the country, we find new wants, requiring for their satisfaction the products of distant lands and climes. In place of the old local and national seclusion and self-sufficiency, we have intercourse in every direction, universal inter-dependence of nations. And as in material, so also in intellectual production. The intellectual creations of individual nations become common property."* [1]
>
> Marx and Engels. (1848) The Communist Manifesto

> *"This is our world now... the world of the electron and the switch, the beauty of the baud."* [2]
>
> The Mentor. (1986) The Conscience of a Hacker

Our world right now

We are no longer defined as a person by what we think. We are defined by what we use, what we buy. We are defined by what society thinks of us and what marketing sells us. The products we surround ourselves with are a definition of our lifestyle.

Computer companies know about our needs for self-fulfillment and social acceptance. They use it every day to sell more, to sell faster, in ways to define ourselves more to their image. We live a marketing defined lifestyle. The idea of throwing information from a computer to the tablet, from there to the phone and from the phone to the television comes to us on television as the way to live. The only way to live.

At the same time, technological, trendy and savvy geeks build their own world through electronics and computer systems, with their own functions, hacking away into electronic components to build their own machines, no longer needing the multinational corporations to determine the style for their lives.

Companies are run from the servers. Integration is everything. The Chief Information Officer (CIO) can t pull the plug on any server without being sacked by the Chief Executive Officer (CEO). Computers hold more information about ourselves and our companies than we ever imagined being possible.

From our computers, through our interconnected smartphones, we can access locally our music player and we are able to share our lives with anyone in the entire world. No boundaries, no supervision, only the social need to interconnect.

One can hold an entire collection of books in a smartphone and still have space for mp3 music files to go along. Every electronic device seems to find a way to communicate to the others related to him only to pass an email or to program some feature.

---

[1] Karl Marx and Friedrich Engels. (1848)" The Communist Manifesto" Retrieved on: December 6th 2013 http://www.marxists.org/archive/marx/works/1848/communist-manifesto/

[2] The Mentor. (1986) "The Conscience of a Hacker" © Copyleft 1985-2012, Phrack Magazine. Retrieved on: December 5th 2013 http://www.phrack.org/issues.html?issue=7&id=3#article

Systems are interconnected, over automated, over controlling, under controlled. We have computer controlled everything.[3] Our computers are our intermediary to our everyday life. Computers control the sprinklers, our crops, the highway, our money, the time and our water. Computers even control the electricity that juices them and our nuclear plants that produce the juice.

> "*In this world we have created? We made it on our own.*"[4]

Have we ever stopped to think what would happen if a computer got a cold? What would happen if all our computers got a virus and stopped working? A transmuted disease that would spread across the planet and wipe out the way we live today? Is it controllable? Can we predict its outcome? Is it even possible? Is it even feasible? Is it even a problem?

Is it possible for us to obliterate ourselves from the universe by means of computer misuse?

What are the opportunities available for total failure as humanity through the use of computers?

The nay sayers

There are those who will say there is no way for us to do a global wipeout by means of computer threat. The *nay sayers* tend to look at the problem as the skeptics look at globalization. Globalization is nothing new and so there is nothing new to see, so... move along.

The internet connected toaster and microwave have no way to attack me in my kitchen and the state-controlled systems, of which life depends, have enough safeguards to protect us from human error or terrorists. Physical access to the infrastructure is still needed to affect the physical environment, so... let's beef up physical security.

The *nay sayer* will advocate that the power of total annihilation is still a problem of the states and that states still have in their hands the monopoly of real threat. The states have everything under control and there are no unknown or incalculable risks, they just need to adapt to the new threat with legislative reforms and more security in order for you to keep your freedom.

The skeptics will say states have no real interest in total annihilation, that this computer *nerdiness* is just new technology and the governing bodies will not allow chaos to happen through any technology.

States will look at computer technology as a means to get war to the doorstep of those they want to bind to their decisions. The Internet and computer software are just new technologies ready to be weaponized and used in favor of the state's policy.

Carl von Clausewitz defines war as *an act of violence to compel our enemy to do our will.*"[5]. From the war point of view this means that computer technology is good for espionage, sabotage and subversion, but not for direct destruction. The mere idea that there will be a technology only war is as ludicrous as the idea of a full-scale nuclear war.

---

[3] Carlin, George. (2004) "Modern Man", Retrieved on: December 8th 2013 http://www.openculture.com/2011/05/george_carlin_the_modern_man_in_three_minutes.html

[4] Freddie Mercury & Brian May. (1984) "The Works". Retrieved on: December 8th 2013 http://www.youtube.com/watch?v=OM0g-7sZeSo

[5] General Carl von Clausewitz. (1874) "On war" (Translated by Colonel J.J.. Graham). Retrieved on: December 6h 2013 http://www.gutenberg.org/files/1946/1946-h/1946-h.htm

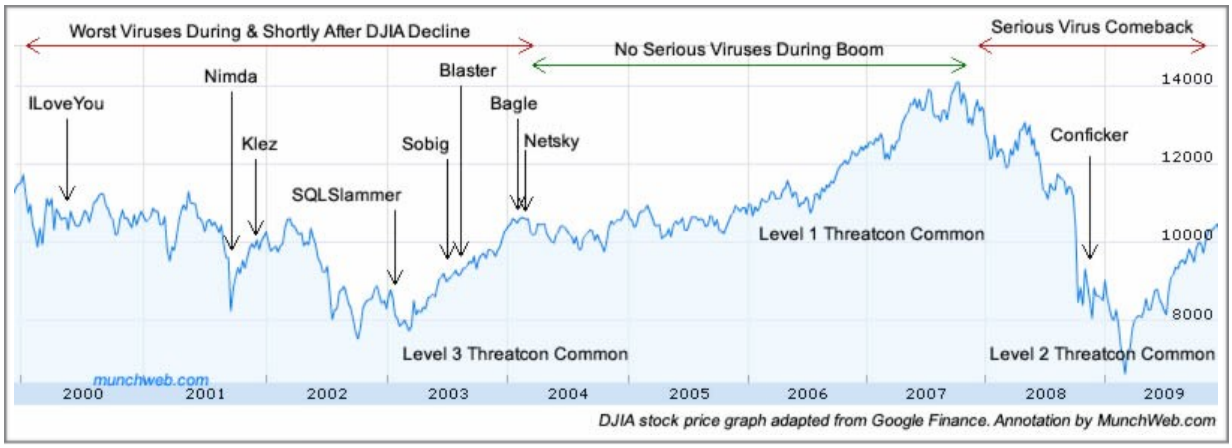
> *"One of the staff at my school (King s College, London) recently published a paper that used Clausewitzian definitions of war to declaim that there has been no cyberwar, cyberwar is not happening now, and cyberwar is unlikely to occur in the future. Of course it is easy to prove a point if you control the definitions and I will stipulate that the idea of two nations engaging in purely network and computer based attacks would result in nothing but fodder for cyber pundits and tech journalists."* [6]

There has always been war because any war is economical, by definition, even if they tell you otherwise. Look at the cold war: did you see any holes full of bodies? No? There you have it.

We can wage war at your backyard, and you won't even notice the gore, and that's how good we are. Of course war has its price, so don't bother with any oil price changes. It will come down. Eventually...

The outcome of war has been death and economic distress, but data says highest computer threats have appeared after economic difficulties, and not before. This is illustrated by the figure bellow[7].

> *"The highest Threatcon level ever has been Level 3 which occurred multiple times in 2003 and 2004, but has not occurred since. The Dow Jones stock index bottomed in 2003 after a downward trend that lasted 3 years, so this is exactly when we would expect higher Threatcon ratings.* [8]



So, if the computer threats are an effect of poor economic performance and not the cause, why worry? We have a cause; we have an effect. All we need to do to maintain the effect from happening is not letting the cause occur.

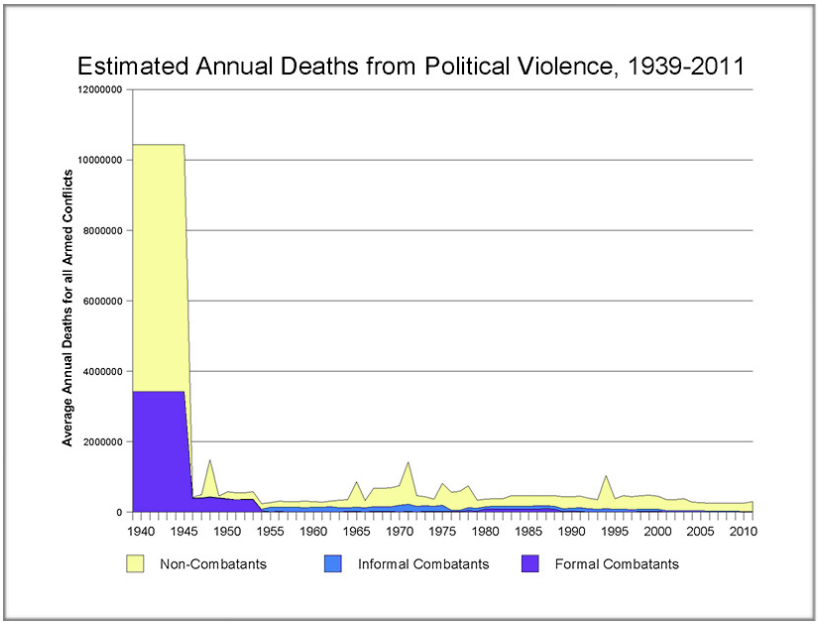
---

[6] Richard Stiennon. (2011), "There is no cyber war the same way there is no nuclear war" Forbes. Retrieved on: December 6th 2013 http://www.forbes.com/sites/richardstiennon/2011/11/03/there-is-no-cyber-war-the-same-way-there-is-no-nuclear-war/

[7] Chris Munch. (2009)" Computer Virus Increase Driven by Weak Economy? Top Trojans & Worms Follow Stock Market Declines" © 2013 MunchWeb. Retrieved on: December 6th 2013 http://munchweb.com/computer-viruses-economy

[8] Chris Munch. (2009)" Computer Virus Increase Driven by Weak Economy? Top Trojans & Worms Follow Stock Market Declines" © 2013 MunchWeb. Retrieved on: December 6th 2013 http://munchweb.com/computer-viruses-economy

We are still to see the death of population by the thousands as the result of computer catastrophe. And even if we see it, it will never be to the size of World War II (WWII). No other humanitarian event has even sized to the WWII proportion after it, as the bellow graphical representation shows.[9]



If we couldn t obliterate ourselves from the face of the earth then, why would we be able to do it now with the keyboard.

If nations need to wage war, they will still do so in the traditional way. Computers are nothing better than tools for the bean counters in the back lines. Forget about it. Just go on and like our page on Facebook.

> *Modern, professional warfare conducted by the full coterie of the world's most technologically and economically advanced countries has been estimated to have resulted in the deaths of about 24 million formal combatants and nearly 50 million non-combatants over the seven year duration of the Second World War (the graph simply averages the estimated total global deaths of the war over the seven-year span).*"[10]

The accusation that computer companies and software developers are the origin of computer chaos is the fabulation of hillbillies and yahoos. This narrative that goes around that computer companies and software antivirus developers create the virus or hype their effects to sell more antivirus is infamous. This was the idea behind the investigation of the H1N1 virus vaccine and see where they have taken it. They spent your hard-earned money on these parliamentary investigations and got you nothing in return.

[9] Center for Systemic Peace (2013)" Global Conflict Trends" Center for Systemic Peace. Retrieve on: December 6th 2013 http://www.systemicpeace.org/conflict.htm

[10] Center for Systemic Peace (2013)" Global Conflict Trends" Center for Systemic Peace. Retrieve on: December 6th 2013 http://www.systemicpeace.org/conflict.htm

> *Just about a year ago the Parliamentary Assembly of the Council of Europe announced a bizarre inquiry. They launched an investigation to establish to what extent pharmaceutical companies connived throughout 2009 to gin up a global panic about swine flu."* [11]

Who would even imagine that an economic player would try to gain a profit over a self-fulfilling prophecy? It's ludicrous to think that companies would create a virus or leave a backdoor on their own software, vaccinate and correct the issue for themselves and their partners before it was outed. Why would a company hype a problem just to sell protection for profit? This would only rise in-satisfaction in their customers and point all the guilt to their side.

> *If an antivirus conspiracy existed on a global level, I'm certain that the various law enforcement agencies around the world would have already found a money trail leading from antivirus companies to worm and virus authors."* [12]

This kind of theories would look like racketeering schemes and would be discovered quickly just by analyzing the money flow. People invent these theories to sell doomsday bunkers, essays, news and get a profit from the people that believe anything they read in the internet. End of story.

The doomsayers

The doomsayers are those that believe that the end of the world is near, and it will arrive in chariots of fire groomed by the internet. They can cite daily news that shows how the world could end by the turning of a switch or the press of a button. The risk of a cyber-something backfiring or intentionally bringing havoc on society on a global scale and with unpredictable results is always present.

Uncontrolled cyberwar action can result in total doom, and this is the ultimate humanity challenge. We should look at it as another war: arm yourself to the teeth so your nearest neighbor thinks twice before trying to take you down. Because the internet makes you as close to your neighbor as you can be to the country in the far end of the world, everyone is a potential target or assailant. You might not even be able to know if the attack comes for you or just knocked at your door by mistake.

Cybercrime and hacktivists explore every defect of the system to whatever objectives. Because there is no control over the geographical whereabouts of the attacker and the state control is based on physical borders and force, undermining these initiatives takes time and, in the meanwhile, the attacker may move to another point.

Computer menaces grow by the day, and we are not ready to deal with them. Antivirus effort depends on coordination of multiple powers and each time we look there are more threats. Conspiracy theorists believe that these threats are left behind by software companies in order to allow for world domination.

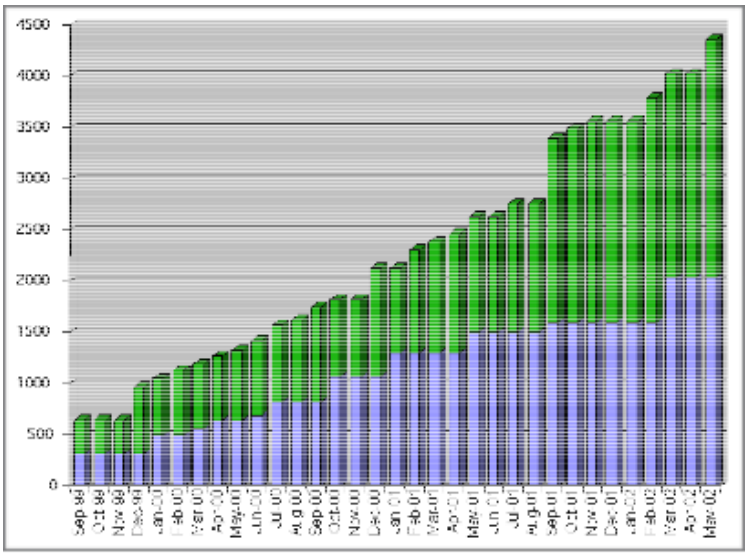
---

[11] Arthur Caplan. (2011)" Did the Vaccine Industry Manipulate the WHO to Sell H1N1 Shots?" Science Progress, Retrieved on: December 6th 2013 http://scienceprogress.org/2011/01/did-the-vaccine-industry-manipulate-the-who-to-sell-h1n1-shots/

[12] Jonathan Yarden. (2005)" Why there is no global antivirus software conspiracy" TechRepublic © 2013 CBS Interactive. Retrieved on: December 8h 2013 http://www.techrepublic.com/article/why-there-is-no-global-antivirus-software-conspiracy/

The threat assessment registers new possible holes and reassesses old ones every day. The growth is horrendous, as illustrated in the graphic bellow[6], and there is no way we can cope with this our own.

> *The CVE Web site now tracks some 4,350 uniquely named vulnerabilities and exposures, which includes the current CVE List, recently added legacy candidates, and the ongoing generation of new candidates from recent discoveries."* [13]



We are doomed. If a kid can play War Games with a computer and place the world in danger by mistake, imagine what can happen if the states decide to weaponize a computer virus.

> *«It s like biological weapons; when you set one off in one place, it affects many others.» Cyber-weapons of the magnitude of Flame are just as destructive. «The world is just so interconnected today, and the viruses that attack one power plant puts them all at risk,» Kaspersky said."* [14]

We are losing our liberty to all this efficacy and efficiency provided by computers and the all accessing networks. The internet is full of tubes and nothing we do on the tubes comes without a price.

> *"Any sound that Winston made, above the level of a very low whisper, would be picked up by it, moreover, so long as he remained within the field of vision which the metal plaque commanded, he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment."* [15]

What was a visionary romance of Eric Arthur Blair's pseudonym George Orwell is now a reality not yet completed but already foreseeable. Like the incomplete Death Star on George Lucas'

---

[13] Robert Martin, Steven Christey and David Baker. (2002)" A Progress Report on the CVE Initiative" The MITRE Corporation. Retrieved on: http://cve.mitre.org/docs/docs-2002/prog-rpt_06-02/

[14] David Shamah. (2012)" Latest viruses could mean 'end of world as we know it, 'says man who discovered Flame" The Times of Israel. Retrieved on: December 7h 2013 http://www.timesofisrael.com/experts-we-lost-the-cyber-war-now-were-in-the-era-of-cyber-terror/

[15] George Orwell (Eric A. Blair). (1949) "Ninety Eighty Four"

Empires Strikes Back movie, cyberwar centers are now a fully operational weapon to impose the rule inside and outside the physical frontiers.

The social networks based on interconnected computers are now the international playground for a new school of spies. Trading cards are no longer exchanged in check point Charlie, but underneath the ocean over the fiber cable backbone of the Internet.

In the year 2013 we finally got a taste of the respect state-nations institutions have for national and foreign citizens. A contractor for the United States of America's National Security Agency (NSA) got fed up with all he was looking at and decided to spill the beans. During some time, this outsourcer used is internal access and social engineering skills to add sensitive information to a cache he would latter deliver to a journalist from the United Kingdom's newspaper The Guardian.

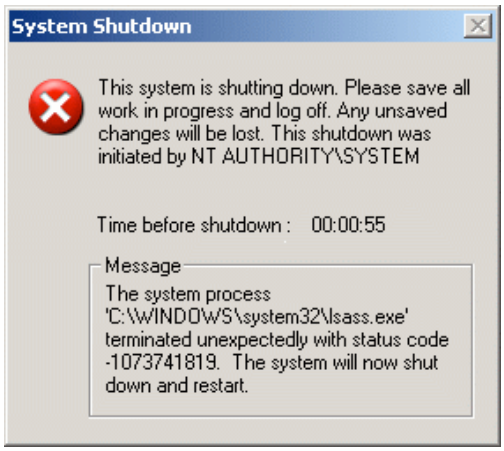
> "*US internet companies, their co-operation with the NSA exposed by Snowden's documents, fear a worldwide consumer backlash, and claim they were forced into co-operation by the law.*
>
> *Much of the NSA s defence is that the public should be unconcerned, summed up by the dictum: If you have nothing to hide, you have nothing to fear.*" [16]

We can only arm ourselves not to engross the number of computer zombies with our own internet capable equipments. We should buy anti-virus, learn cryptography, configure a firewall and install anti-malware. Even better, our best choice of survival is to run to the hills and build a doomsday bunker to save ourselves and our families.

[16] Ewen Macaskill and Gabriel Dance. (2013) © The Guardian. Retrieved on: December 4th 2013 http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Back to earth

In the beginning of 2004 Microsoft issued a security bulletin for a remote code execution vulnerability[17] that was abused latter by a computer virus known as the Sasser worm. The Sasser computer virus became widespread by the nature of its code. One of its symptoms can be seen in the image below where the system executable *lsass.exe* would not be able to close, hence the name Sasser.



As a result, infected computers had to be intervened. It is not possible to preview or calculate the costs of a computer being abused from vulnerabilities that were not properly patched.

> *Computer systems of Sampo, Finland's third largest bank, RailCorp in Australia and various other networks were hard hit by Sasser, resulting in operational problems."* [18]

Created by a German adolescent just turned 18, the virus used a vulnerability on a connection port to propagate itself to the next computer. After infecting the computer, it would jump to the next computers found on the network available to the same exploit method. This port is almost always available in Windows, so a new unknown vulnerability can already be exploring it without our knowledge.

> *Sasser wrought havoc when the Windows worm struck in May 2004, swamping net links and making computers unusable. Jaschan had admitted to creating the worm at the beginning of his trial on Tuesday, reiterating a confession to authorities at the time of his arrest in May 2004."* [19]
>
> *In the UK, the worm shut down the computers of the Maritime and Coastguard Agency, with staff returning to manual map reading."* [20]

[17] Microsoft Corporation (2004)" Microsoft Security Bulletin MS04-011" Issued: April 13, 2004, Retrieved on: December 5th 2013 http://technet.microsoft.com/en-us/security/bulletin/ms04-011

[18] John Leyden. (2004)" Sasser worm creates havoc. Blaster Mk II hits railways and banks" © 2004 The Register. Retrieved on: December 4th 2013 http://www.theregister.co.uk/2004/05/04/sasser_worm

[19] (2005) BBC. Retrieved on: December 7th 2013 http://news.bbc.co.uk/2/hi/technology/4659329.stm

[20] (2005) BBC. Retrieved on: December 7th 2013 http://news.bbc.co.uk/2/hi/technology/4659329.stm

> *Unlike many other viruses, Sasser made its way from computer to computer without help from users. It got into Windows computers by exploiting a programming bug in the operating system."* [21]

It is not possible to effectively determine if a computer virus was totally eliminated from all the interconnected computers. One can only state that the virus signature is no longer found on the checked computers. This is a logical limitation, not a technical one.

We don't even know if a mutated version or a descendant created by someone that fancied the original code is not already making the rounds using some zero days exploit and zombifying half of the computers in the Internet.

This was not the first time a virus by a computer science student went amok, nor will it be the last. Governments are looking at legislative measures to reduce the prevalence of something the ink of law can t affect.

> *The threat is really very easy to understand. If there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage to the economy. What could happen? Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. 911 emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled. If that major attack comes at a time when we are at war, it could put our forces at great risk by having their logistics system fail."* [22]

Governments are now worried about the potential of this computer risk becoming a catastrophic economical event, but never considering it as a risk of incalculable impact on the people from the result of their own mishaps.

For years, a weak password was unknowingly the real highest threat in the nuclear cold war years.

> *Those [missiles] in the U.S. that had been fitted with the devices, such as ones in the Minuteman Silos, were installed under the close scrutiny of Robert McNamara, JFK's Secretary of Defence. However, The Strategic Air Command greatly resented McNamara's presence and almost as soon as he left, the code to launch the missile's, all 50 of them, was set to 00000000."* [23]

Governments are more worried about weaponized virus from other countries or terrorists then they are about their mismanagement.[24] Governments worry more about cybercrime and how it can disrupt economical activities than the end of the world at the hands of stupidity and technological illiteracy.[25]

---

[21] (2005) BBC. Retrieved on: December 7th 2013 http://news.bbc.co.uk/2/hi/technology/4659329.stm

[22] Cyber Security: The Challenges Facing Our Nation in Critical Infrastructure Protection: Hearing before Subcomm. on Tech., Info. Policy, Intergovernmental Relations and the Census of the H. Comm. on Gov't Reform, 108th Cong. 13 (2003) (statement of Richard A. Clarke, former Special Advisor to the President for Cyberspace Security)

[23] Karl Smallwood. (2013) Gizmodo Gawker Media. Retrieved on: December 6th 2013 http://gizmodo.com/for-20-years-the-nuclear-launch-code-at-us-minuteman-si-1473483587

[24] Brian B. Kelly. (2012) "Investing in a Centralized Cybersecurity Infrastructure: Why "Hacktivism" Can and Should Influence Cybersecurity Reform" Boston University Law Review Vol. 92:1663

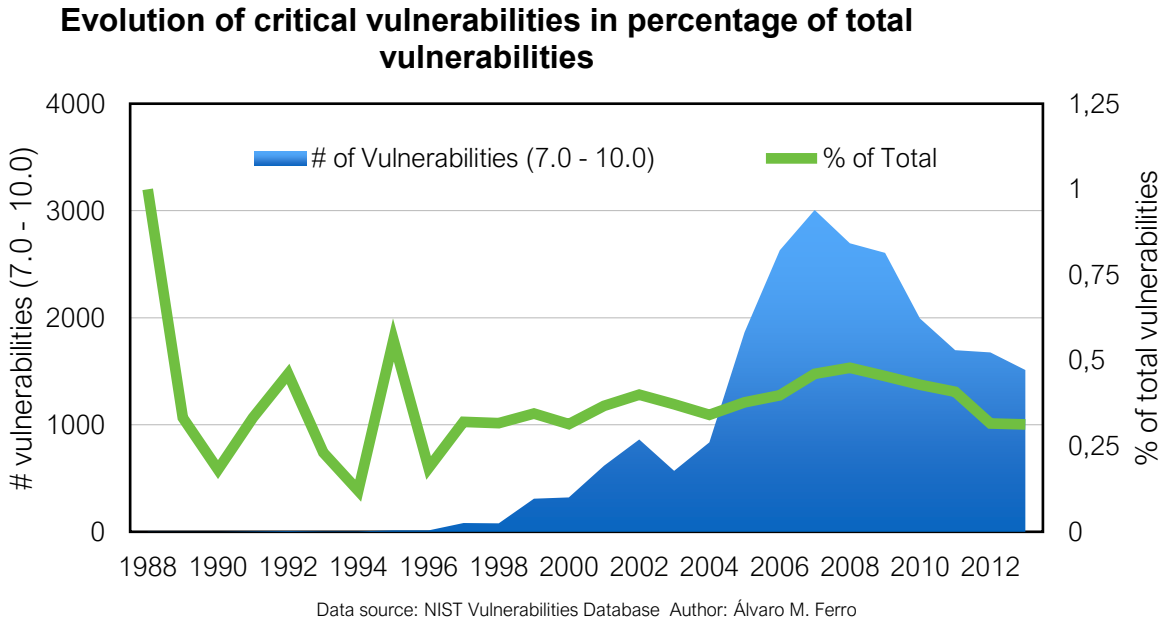
[25] John Arquilla and David Ronfeldt.(1993) "Cyberwar is coming!" Comparative Strategy, Vol. 12, No. 2, Spring 1993, pp. 141-165. Retrieved on: December 6th 2013 http://www.rand.org/pubs/reprints/RP223.html

> "*Western governments are close to an agreement that would put sensitive cyber security technologies on the same footing as regular armaments under one of the world s main agreements on weaponry export control.*"[26]

The cost of threats becoming reality is mainly calculated not in loss of life, but in loss of profit. The interconnected economy needs to be online and work at its fast pace. When computer cycles are busy running rogue code that is looking for its next victim, they are not turning profit. This is bad, but not catastrophically bad.

The trend seems to say that the market has been able to stabilize the trend of the ever-growing threat number of known vulnerabilities, no pun intended. The trend of high threat vulnerabilities is lowering in number, but it is still not time to rest. Data available on National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD)[27] tells us this about remotely exploitable software flaws.

The graphic plotted for this essay and shown below gathers information on vulnerabilities on software that match a CVSS Base Score between 7.0 to 10.0 on a maximum of 10[28], but counts only the vulnerabilities exploitable remotely. Although the numbers stopped growing, the number of threats that score the highest is not going away and still amounts for almost one third of all vulnerabilities found. One third of the vulnerabilities registered are a risk to interconnected systems that have the vulnerability.



[26] Sam Jones. (2013) © The Financial Times Ltd 2013. Retrieved on: December 4th 2013 http://www.ft.com/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html#axzz2munnXKCn

[27] Data obtained from the National Vulnerability Database. Retrieved on: December 8th 2013 http://web.nvd.nist.gov/view/vuln/statistics-results?cves=on&query=&cwe_id=&pub_date_start_month=-1&pub_date_start_year=-1&pub_date_end_month=-1&pub_date_end_year=-1&mod_date_start_month=-1&mod_date_start_year=-1&mod_date_end_month=-1&mod_date_end_year=-1&cvss_sev_base=HIGH&cvss_av=NETWORK&cvss_ac=&cvss_au=&cvss_c=&cvss_i=&cvss_a=

[28] FIRST is the Forum of Incident Response and Security Teams. (2007) Common Vulnerability Scoring System. Retrieved on: December 8th 2013 http://www.first.org/cvss

While in 1988 the total number of highest threat vulnerabilities registered on the United States of America National Vulnerability Database was as low as one, it still amounted to a total of 100% of all menaces of the highest score registered affecting interconnected computers.[29]

The highest classified flaws that spiked when Stuxnet virus was around are now trending down. This only means we don't yet know about the other vulnerabilities not yet found.

> *Three years after it was discovered, Stuxnet, the first publicly disclosed cyberweapon, continues to baffle military strategists, computer security experts, political decision-makers, and the general public."* [30]

The knowledge that a threat as Stuxnet' younger brother was already running in the infected systems as a prerequisite for Stuxnet to execute correctly when its older brother was finally detected has perplexed computer experts. Stuxnet origin is still not known, but it is mainly being attributed to a United States of America and Israel s effort to destroy the Iranian nuclear program. The objective of the pair of viruses known as Stuxnet was to change the behavior of the uranium-enrichment centrifuges covertly, without giving its position way and allowing to continually sabotage the program.

> Stuxnet-inspired attackers will not necessarily place the same emphasis on disguise; they may want victims to know that they are under cyberattack and perhaps even want to publicly claim credit for it."[31]

The expectation that some kind of mutation might still be around may give us an idea of how big a threat a computer might become.

Computer controlled critical infrastructures are now the main target for computer sabotage of the weaponized virus kind, but has with all the computer virus, the real problem is not only the main target, but the number of problems it spreads to all the other systems it has contact with.

> *Computerized hospital equipment is increasingly vulnerable to malware infections, according to participants in a recent government panel. These infections can clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable."* [32]

Dr. Mark Gasson, from the University of Reading, had a medical chip inserted in his hand which was then infected with a virus by coming in contact with an infected device. The implant was not

---

[29] Data for the graph obtained from the National Vulnerability Database. Retrieved on: December 8th 2013 http://web.nvd.nist.gov/view/vuln/statistics-results?cves=on&query=&cwe_id=&pub_date_start_month=-1&pub_date_start_year=-1&pub_date_end_month=-1&pub_date_end_year=-1&mod_date_start_month=-1&mod_date_start_year=-1&mod_date_end_month=-1&mod_date_end_year=-1&cvss_sev_base=HIGH&cvss_av=NETWORK&cvss_ac=&cvss_au=&cvss_c=&cvss_i=&cvss_a=

[30] Ralph Langner. (2013) http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack#sthash.IErffk1M.dpuf

[31] Ralph Langner. (2013) http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack#sthash.IErffk1M.dpuf

[32] David Talbot. (2012) Computer Viruses Are "Rampant" on Medical Devices in Hospitals MIT Technology Review. Retrieved on: December 7th 2013 http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

of the medical kind, but rather an identification tag that allowed the implanted subject to unlock security doors and his computer devices.[33]

The process of identifying someone via one such device implies data exchange from the implanted machine to the security device that identifies it, and if the code running in one of the devices is vulnerable, the virus can jump from one to the other.

> *Implanted technology has become increasingly common in the United States, where medical alert bracelets can be scanned to bring up a patient's medical history.*"[34]

[33] David Talbot. (2012) Computer Viruses Are "Rampant" on Medical Devices in Hospitals MIT Technology Review. Retrieved on: December 7th 2013 http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

[34] Nick Collins. (2010)" Scientist 'infected' with computer virus" © Copyright of Telegraph Media Group Limited 2013, Retrieved on: December 8th 2013 http://www.telegraph.co.uk/technology/news/7766627/Scientist-infected-with-computer-virus.html

Are interconnected computers a global risk to the society?

> *"The theory of world risk society maintains, however, that modern societies are shaped by new kinds of risks, that their foundations are shaken by the global anticipation of global catastrophes."* [35]

Ulrich Beck tells us that the perception of global risk can be characterized by delocalization, incalculableness and non-compensability. [36]

Due to the prevalence of computerized everything in the world, it is not just a problem of computers, but of everything that a logical device exchanges data with. Add up the interconnectivity and the freedom of data to roam the world at the speed of the electron to the equation and you realize that there is no spatial confinement whatsoever possible to such a threat. A virus produced to attack on Iran[37] can easily get into your hospital equipment[38].

The amounting of known vulnerabilities [39] and threats [40] we known have no relation to the unknown possible zero-day vulnerabilities and unknown threats that may already started being exchanged. This makes it impossible to calculate what would be the impact of someone actively trying to take advantage of them.

By the examples gathered for this essay or just by reading the news on the Internet, the ramifications of such events and the multiplicity of places they might occur at the same time, it seems impossible to predict the impact for the known threats and even more for the unknown threats.

The knowledge that one such threat[41] could be years roaming and be abused until it is first identified, removes any notion of predictability and therefore no amount of calculation can be done to prepare a mutualization of a compensation if such a risk could become a reality.

In the worst-case scenario, one such roaming menace could be used by an extremist to make sure we know he exists and what are his demands, making interconnected computers the menace.

---

[35] Ulrich Beck. (2006) "Living in the world risk society" Economy and Society Volume 35 Number 3 August 2006: 329 345

[36] Ulrich Beck. (2006) "Living in the world risk society" Economy and Society Volume 35 Number 3 August 2006: 329 345

[37] Ralph Langner. (2013) http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack#sthash.IErffk1M.dpuf

[38] David Talbot. (2012) Computer Viruses Are "Rampant" on Medical Devices in Hospitals MIT Technology Review. Retrieved on: December 7th 2013 http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

[39] Data obtained from the National Vulnerability Database. Retrieved on: December 8th 2013 http://web.nvd.nist.gov/view/vuln/statistics-results?cves=on&query=&cwe_id=&pub_date_start_month=-1&pub_date_start_year=-1&pub_date_end_month=-1&pub_date_end_year=-1&mod_date_start_month=-1&mod_date_start_year=-1&mod_date_end_month=-1&mod_date_end_year=-1&cvss_sev_base=HIGH&cvss_av=NETWORK&cvss_ac=&cvss_au=&cvss_c=&cvss_i=&cvss_a=

[40] Robert Martin, Steven Christey and David Baker. (2002)" A Progress Report on the CVE Initiative" The MITRE Corporation. Retrieved on: http://cve.mitre.org/docs/docs-2002/prog-rpt_06-02/

[41] Ralph Langner. (2013) http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack#sthash.IErffk1M.dpuf

In a case that all the computers got a virus that would render them useless, these might not affect anyone but the ones dependent on computers. It's still to be proved that one such event would impact directly on the non-western civilization.

This does not mean that third world countries that have none or limited access to interconnected technology would not be affected. It just means we cannot determine how they would be affected. It means that one such event would only leave untouched the already untouched society only if the risk would impact only the computers. Taking into account the threat to a computerized system on a nuclear power plant, the whole scenario can change and risk will affect even the unconnected world.

It is still the cautious old man way that subsist as our last chance of control and security warranty. When confronted by a history of things going wrong due to technology mishaps, the old man tends to look at technologies suspiciously. Like in the minuteman silos, they don't relax the human control over critical equipment. They tend to cut the technological ties between machines, making man the single point of failure.

Men are much more adaptable, and technology gave them a way to have control over humans. One can only propose that our failure as humanity has been exposed by such cases as Wikileaks and Snowden[42].

The continued abuse of computers to control us has been the issue, not our loss of control over the interconnected computer. Our control of interconnected computers has proven that we humans are the reason of our own doom and not the other way around.

> "*There is no shortage of whistleblowers," as the counter-experts to the zero-risk pronouncements are judiciously termed. And the law also holds universally that after the catastrophe, the warnings of counter-experts are proved right. Moreover, the end of one catastrophe is merely the prelude to another.*" [43]

[42] Ewen Macaskill and Gabriel Dance. (2013) © The Guardian. Retrieved on: December 4th 2013 http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

[43] Ulrich Beck. (2008) "Critical Theory of World Risk Society: A Cosmopolitan Vision" Constellations Volume 16, No 1, 2009. The Author. Journal compilation, Blackwell Publishing Ltd.