

Casey Alt

Viral Load. The Fantastic Rhetorical Power of the Computer Virus in the Post-9/11 Political Landscape

There is something profoundly quixotic in attempting to write a history of the computer virus. One would think that, given the immense rhetorical power of computer viruses in America throughout the past decade, it would be relatively easy to create a concise cultural history of such a phenomenon. One might imagine that, given the hundreds of reported computer viruses that have plagued the world's information systems, that there would be a wealth of abundantly populated archives and a vigorous community of research around such a topic. One could even suppose that governments would enthusiastically support the open discussion of such historical research as a means for increasing public awareness of the nature and risks of computer viruses.

While the above assumptions are all entirely reasonable, none of them happen to be true. Instead, what exists is a vast assortment of ambiguous and unsubstantiated details that affords little, if any, research or analysis. This is not to say that there is no documentation of periodic computer virus infection events. On the contrary, a simple search of most online news portals will reveal thousands of journalistic accounts of computer virus outbreaks. However, the vast majority of these reports provide little beyond sensationalist statistics and superficial descriptions of the various incidents. Under closer inspection, even the statistics themselves become questionable.

The two indispensable elements in any report of computer virus activity consist of an estimate of the numbers of infected computers and an estimate of the financial cost of the outbreak. As it turns out, both of these measures are often problematic. With regard to calculations of the numbers of infected computers, nearly all assessments are of one of two types: (1) projected estimates based on small anecdotal subsamples of the number of infected machines at certain local sites, and (2) projected estimates of the extent of the outbreak based on statistics from the antivirus software

companies themselves. While the first estimates are always incomplete, the second are even more dubious, considering that it is always in the best interest of antivirus software companies to present the highest possible infection rates. Additionally, many organizations, primarily financial institutions, refuse to disclose their virus infection rates, as it is tantamount to publicly admitting technological vulnerabilities and/or irresponsible information security practices.

When it comes to calculating the financial damage caused by large-scale computer virus outbreaks, the results are equally nebulous. Journalists often rely on third-party consulting firms, such as the California-based company Computer Economics, to assess the relative costs of computer virus outbreaks. Of course, these cost estimates also depend primarily upon figures provided by antivirus companies. In an article entitled »Lies, damned lies and anti-virus statistics«, John Leyden of *The Register* reported that when Computer Economics stated in its annual assessment of worldwide computer virus damage for 2001 that yearly damage estimates had decreased by 23% from US\$ 17.1 billion in 2000 to US\$ 13.2 billion, antivirus companies, such as MessageLabs and Sophos, vehemently attacked the figure as a »guesstimate« and poked numerous holes in the company's methodology.¹ In particular, Leyden quoted Alex Shipp, chief antivirus technologist from MessageLabs – a British firm specializing in email security, who argued that »users are unable to estimate the damage a virus outbreak might cause their own company (...) so how does a third party get the figure?«² Despite claims by Computer Economics that its consultants work closely with antivirus companies to assure the most accurate financial estimates, executives from both MessageLabs and Sophos, two of the leading international email security corporations, denied having ever been contacted by Computer Economics to provide statistics on infection rates. *The Register* has also questioned the accuracy Computer Economics figures by claiming that »patching systems is, after all, a core part of the work of most [system, C.A.] administrators«, so where, they argue, is all the additional expense derived?

A March 2002 report from the Institute for Security Technology Studies at Dartmouth College echoed many of *The Register*'s concerns regarding »the validity and scientific rigor« of Computer Economics' numbers, noting that »the company has, so far, been reluctant to disclose details of its methodology and sources relating to the estimates«.³ Among its many criticisms of Computer Economics' projections, the report mentioned the following:

At the top of the list is the point that no reliable microeconomic data on computer viruses or worms is available from which to make assumptions on a global scale. Moreover, even if the economic impact of a virus or worm could be accurately measured for individual infections, this would not necessarily

transfer to virus outbreaks as a whole because each case is different. In addition, too many factors connected to viruses and worms, such as the number of infections for each virus, remain disputed. Finally, critics emphasize that clean-up costs and lost productivity are such subjective criteria that no coherent tabulation of economic costs can be based on them.⁴

The report continued to elaborate on the lack of reliability in approximating the financial impact of computer virus and worm outbreaks, concluding that, »while available estimates of global economic costs of viruses and worms may give a general indication of the relative costs of viruses, they should be viewed with caution. There is currently no consistent and reliable method to assess the micro- or macroeconomic impact of a virus or worm.«⁵

One might suspect that it would be in the best interest of U.S. governmental agencies to have a better handle on such assessments. Traditionally, the heavily government-funded Carnegie Mellon University's Computer Emergency Readiness Team Coordination Center (CERT/CC) was one of the few relatively independent organizations to publish self-reported incidents of computer infections and attacks. However, in 2003, even CERT/CC abandoned their attempt to track such statistics, claiming that

given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks. Therefore, as of 2004, we will no longer publish the number of incidents reported.⁶

George Smith, senior fellow at GlobalSecurity.org and founder of the popular Crypt Newsletter,⁷ has demonstrated even more egregious lapses in the ability of U.S. security officials to accurately monitor computer security risks. In an article entitled »An Electronic Pearl Harbor? Not Likely« in the Fall 1998 issue of *Issues in Science and Technology*, Smith cited a number of examples demonstrating the U.S. Federal Bureau of Investigation's lack of intelligence in all things computer viral. According to Smith, a December 1996 issue of the FBI's *Law Enforcement Bulletin*, entitled »Computer Crime: An Emerging Challenge for Law Enforcement«, featured an article written by researchers from Michigan State and Wichita State universities, in which the article described a number of recent computer virus threats, including an example of »A virus called ›Clinton (...) designed to infect programs, but (...) eradicates itself when it cannot decide which program to infect.«⁸ According to Smith, »both the authors and the FBI were embarrassed to be informed later that there was

no such virus as ›Clinton.‹ It was a joke, as were all the other examples of viruses cited in the article. They had all been originally published in an April Fool's Day column of a computer magazine.«

Smith continued by explaining the degree to which the numbers of general on-line attacks on government institutions have historically often been outrageously inaccurate. In particular, Smith references a figure produced by the U.S. Defense Information Systems Agency (DISA) and the General Accounting Office (GAO) that there were 250.000 intrusions into U.S. Department of Defense (DOD) computers in 1995 alone. Smith explains that the rather staggering figure »has been used as an indicator of computer break-ins at DOD since 1996« and »has shown up literally hundreds of times since then in magazines, newspapers, and reports«, despite the fact that »the figure is not and has never been a real number«. According to Smith,

it is a guess, based on a much smaller number of recorded intrusions in 1995. And the smaller number is usually never mentioned when the alarming figure is cited. At a recent Pentagon press conference, DOD spokesman Kenneth H. Bacon acknowledged that the DISA figure was an estimate and that DISA received reports of about 500 actual incidents in 1995. Because the DISA believed that only 0,2 percent of all intrusions are reported, it multiplied the figure by 500 and came up with 250.000.⁹

Smith further challenged the statistic by consulting Kevin Ziese, a computer scientist who directed one of the DOD hacking investigations in 1995. According to Ziese, even the original DISA statistic of 500 attempted intrusions had been »inflated by instances of legitimate user screwups and unexplained but harmless probes sent to DOD computers«. Yet, in spite of all this, Smith notes, »the figure has been continually misrepresented as a solid metric of intrusions on U.S. military networks and has been very successful in selling the point that the nation's computers are vulnerable to attack«.

The status of reliable research into the history of computer viruses becomes even bleaker when one attempts to study the actual virus programs themselves. Though much of the business of antivirus companies consists of the collection and preservation of computer viruses and worms as a means for recognizing distinct »viral signatures«, it is practically impossible to actually get access to such virus collections. Even if viruses have been »quarantined« on a user's system, the user is often not allowed to access to the quarantined files. The ostensible reason for this high level of secrecy is the claim that open access to computer virus code would result in people writing more computer viruses – a difficult claim for an antivirus company to make given that once they themselves have a copy of a virus then machines running their

antivirus software should already be protected from that virus. Such reasoning is not a far cry from the logic of conservative American political leaders who argue that sex education courses will make children more likely to have sex. A more believable explanation for antivirus companies' unwillingness to release past virus programs is that a large part of their business model is predicated upon their ability to exclusively control stockpiles of past computer virus specimens as closely guarded intellectual property.

None of this absence of archival material is helped by the fact that the concept of a computer virus is itself an ontologically ambiguous category. The majority of so-called »malicious software« entities that have plagued Internet users in the past few years have technically not been viruses but *worms*.¹⁰ Additionally, despite attempts to define clear nosological and epidemiological categories for computer viruses and worms,¹¹ there is still no consistent system for stabilizing the terms themselves, let alone assessing their relative populations. Elizabeth Grosz recently commented during an interview with the editors of *Found Object* journal that part of the reason for the ontological ambiguity of computer viruses is that they are an application of a biological metaphor that is largely indeterminate itself. According to Grosz, »we are as mystified, if not more so, by biological viruses as we are by computer viruses. Perhaps we know even more about computer viruses than we do about biological viruses! The same obscurities are there at the biological level that exists at the computer level (...)«¹²

As Grosz suggests, it is no wonder that computer viruses are so ontologically uncertain, given that their biological namesakes threaten to undermine many of the binarisms that anchor modern Western technoscience, such as distinctions between organic and inorganic, dead and living, matter and form, and sexual and asexual reproduction.

Given this overwhelming miasma of ontological and historical dead-ends, one might assume that the nearly absolute ambiguity surrounding the concept of computer viruses is an indication of its lack of cultural importance. However, such a conclusion would be the exact opposite of what has occurred over the past decade. As I will argue throughout the remainder of this paper, it is precisely such ontological instability and historical invisibility that have elevated computer viruses to one of the most powerful rhetorical forces subtending the post-9/11 American political landscape. Indeed, one might even go so far as to claim that the best way to frame the current American condition is by tracing the ubiquitous lacunae of the slippery and polymorphous computer virus.

The Viral Engine of Late Capitalism

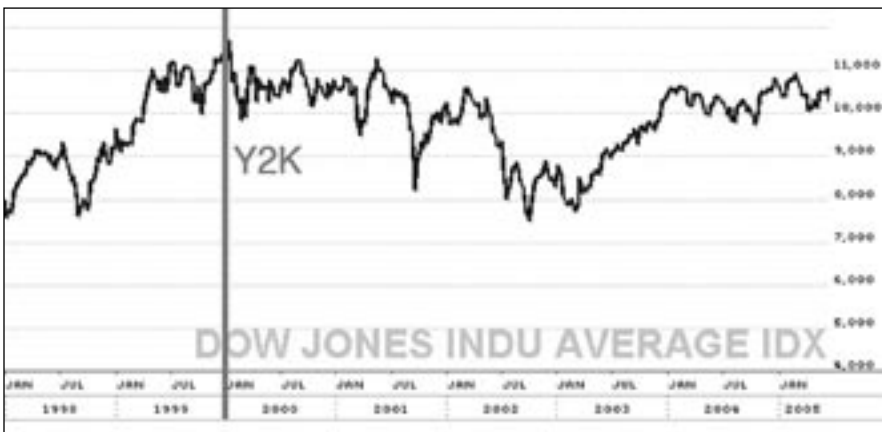
Most economic assessments of computer virus activities focus on the threat that such malicious entities pose to an idealized representation of the global information economy. Within such a system of »friction-free capitalism«, as described by Bill Gates in his 1996 book *The Road Ahead*, any undesirable blockage to the efficient flow of informational goods and services is registered as an implicit loss to producers and consumers everywhere. In his recent article entitled »Digital Monsters, Binary Aliens – Computer Viruses, Capitalism and the Flow of Information«, Jussi Parikka delivers a brilliant analysis that debunks such utopian visions of the contemporary information economy by demonstrating that system vulnerabilities and computer viruses do not detract from the efficient flow of a capitalist information economy but are actually a necessary components of the information economy's own »viral« logic:

However, at the same time as the virus has been articulated as a problem of information capitalism, it has also been captured as a part of that same machinery. Anti-virus software became a lucrative business (...) (V)iruses and worms are not simple anomalies or »enemies« of digital capitalism, but an integral part of it. Hence, capitalism is viral in itself, meaning that its essence lies exactly in its capability of infecting the outside in order to replicate itself. There is no absolute Other for the capitalist logic of expansion. What is crucial is the understanding of this constant double articulation of the virus as a threat *and* an integral part of the contemporary society. The seemingly contradictory themes of the virus as the threat and the essence of capitalism are, in fact, intertwined and operate in sync. The ideas of risk control, safety measures and the construction of the responsible user are thus to be read as integral elements of viral capitalism: with these elements, or discourses, the fear of computer viruses has been turned into a part of the flows of consumer capitalism, products and practices that »buy off« anxiety.¹³

Parikka's argument of the »constant double articulation of the virus as a threat *and* an integral part of the contemporary society« is extremely valuable and accurate, perhaps even more so than he realizes. Parikka points primarily to the proposed viral menace as being incorporated into a larger capitalist information economy via the lucrative antivirus software business; however, one could elaborate on Parikka's assertion by suggesting that precisely what is wrong with Gates' vision of the »friction-free economy« is its representation as a steady-state condition in which no progress can be made or measured. The threat of breaks and stoppages of the system

must *always* exist since they are what cause the system to flow in the first place. Thus, I would push Parikka's case further by claiming that the computer virus industry has not only become an integral component of the global information economy, it has become one of the primary *drivers* of it.

If there were ever a point in which the American information economy might have seemed most »friction-free«, it was immediately prior to the bursting of the so-called »dotcom bubble«. At that time, the American creative information machine seemed to be unstoppable, and the larger U.S. economic outlook had never been more optimistic. In the late 1990s, it seemed as though America had entered a sustained period of nearly effortless prosperity. However, after the turn of the millennium, friction returned to the system with a vengeance. While many analysts have blamed inflated corporate valuations, unbounded consumer optimism, unethical accounting practices, and even the 9/11 terrorist attacks for the bursting of the dotcom bubble, historical data does little to support these arguments. Rather, more sanguine analysts, such as Alan F. Kay, have offered a much simpler picture of things: that much of the steep economic climb, particularly in technology related sectors, was the result of over US\$ 500 billion in global technology investments to prepare for the eventual onslaught of the Y2K bug.¹⁴ It is no coincidence that the Dow Jones Industrial Average peaked immediately after the turn of the millennium in January 2000 or that the technology-heavy American NASDAQ exchange began to decline in March 2000 at the end of the first quarter following the expiration of the Y2K threat:



Graph of the Dow Jones Industrial Average from 01 January 1998-31 January 2005. The red »Y2K« line indicates the market position as of 01 January 2000. (Graph by Casey Alt)



Graph of the NASDAQ Composite Index from 01 January 1998-31 January 2005. The red »Y2K« line indicates the market position as of 01 January 2000. (Graph by Casey Alt)

While one might attribute such a strong correlation to coincidence, let us remember that Y2K compliance investments were not only suggested, they were mandated to many sectors of the economy by the U.S. Securities and Exchange Commission (SEC). In a July 29, 1998, Interpretive Release, entitled »Disclosure of Year 2000 Issues and Consequences by Public Companies, Investment Advisors, Investment Companies and Municipal Securities Issuers«, the SEC required all companies to publicly disclose »(1) the company's state of readiness; (2) the costs to address the company's Y2K issues; (3) the risks of the company's Y2K issues; and (4) the company's contingency plans.«¹⁵ Sensing at the last moment that such strict motivations might not be strong enough, the SEC threatened during the summer of 1999 to force the closure of any brokerage firm that was not Y2K compliant by November 15, 1999, under the justification that »a few firms' lack of readiness could have adverse consequences for countless others«.¹⁶

Since nearly every critical sector of the U.S. economy was required to upgrade their equipment to meet Y2K compliance standards, there is no real way of knowing whether any sort of Y2K catastrophe would have occurred. While the Y2K bug was not a computer virus *per se*, its status as an inherent »accident« within any information system makes it coextensive with Parikka's larger argument about the integral nature of computer viruses in the capitalist information economy. Furthermore, one must remember that one of the most powerful components of fears surrounding the Y2K bug was the related threat of viruses and hackers exploiting Y2K vulnerabilities, and public rhetoric surrounding the urgency of the Y2K often conflated these separate threats. Time and again, the »real« threat of Y2K was not the temporary shut down of a few computer systems, but rather the larger maelstrom of hackers, virus

writers, and other malicious entities who might be poised to take advantage of the moment of weakness – the sum of which was repeatedly packaged in the politically charged phrase »electronic Pearl Harbor«. Smith, who has catalogued hundreds of uses of the phrase since its origination in Alvin and Heidi Toffler's 1993 book *War and Anti-War*,¹⁷ credits President's Clinton's National Coordinator for Security, Infrastructure Protection, and Counter-terrorism on the National Security Council, Richard Clarke, for popularizing the expression in public debates surrounding the Y2K bug.¹⁸ Regardless of whether such widespread fear was justified, the important point is that the fear of it alone was enough to raise the U.S. economy to its highest level in history.

Surprisingly, even in the wake of Y2K, the computer security industry is still one of the few technology sectors showing a steady growth rate. According to a 2004 report from IDC, a leading market intelligence provider to the information technology and telecommunications industries, the security services business is booming:

In research currently carried out by IDC, the market for security-related hardware, software, and services will continue to record a healthy growth rate, in spite of the slowdown experienced by the overall IT sector the profits are expected to grow from just \$17 billion in 2001 to \$45 billion in 2006. Experts believe that the proliferation and widespread use of remote LAN, Internet, extranet/intranet, and wireless access services in the corporate sector is responsible for this stupendous growth. Furthermore, IDC foresees the global market for information security services to reach US\$ 21 billion by the end of 2005, up from US\$ 6.7 billion in 2002.¹⁹

The analysis goes on to explain that in the realm of security software, the U.S. federal government is one of the »biggest employers and spenders«. According the study, the U.S. government »is looking to upgrade its infrastructure to make it more secure from the everyday threat of terrorism« at the cost of US\$ 40.2 billion for fiscal year 2005, an increase of over ten percent from the 2004 budget. A February 4, 2002, article by Elisa Williams of Forbes.com more bluntly diagnosed the recent status of Internet security firms by stating that »while the rest of the tech industry suffers, the computer-security sector exploded after Sept. 11«. ²⁰ In the absence of Y2K, a new engine has emerged to help drive the stagnant U.S. information economy, and, once again, the fuel for such an »explosion« is the rampant fear of computer viruses and their kin.

The Invention of Cyberterrorism

It would be difficult to overstate the rhetorical role that computer viruses and their obligatory retinue of hackers, phishers, and identity thieves have played in constructing the post-9/11 political climate. Immediately following the 9/11 terrorist attacks, President Bush replaced Richard Clarke, who had remained in his position from the Clinton administration, with General Wayne Downing. However, rather than dismissing Clarke outright, the President retained his presence on the National Security Council as the newly created Special Advisor to President for Cyberspace Security.

Given that there was no known »cyber« component to the 9/11 terrorist attacks, it is surprising how much importance the Bush administration has placed on combating »cyberterrorism«. On the same day that the President issued an executive order to establish the Office of Homeland Security on October 8, 2001, the Office of the White House Press Secretary also released a »Fact Sheet on New Counter-Terrorism and CyberSpace Positions«, in which Downing and Clarke summarized their joint missions in protecting the nation's security.²¹ The fact that cyberterrorism was given equal billing with »counter-terrorism« in general in this early document is striking. By comparison, it took over a month for an official »Fact Sheet on Cooperation Against Bioterrorism« to be released on November 13, 2001. Additionally, only eight days after enacting the Executive Order Establishing Office of Homeland Security, President Bush deemed it necessary to issue yet another entirely separate »Executive Order on Critical Information Protection«, which was specifically designed »to ensure protection of information systems for critical infrastructure«.²²

President Bush's emphasis on the importance of preventing cyberterrorism has only intensified in the years after the months following the 9/11 attacks. In his remarks following his signing of the Homeland Security Act on November 25, 2002, President Bush listed the focus on cyberterrorism as the second highest mission for the new department, charging it with the responsibility to »gather and focus all our efforts to face the challenge of cyberterrorism, and the even worse danger of nuclear, chemical, and biological terrorism«.²³ In February 2003, President Bush released a 60-page document ambitiously titled »The National Strategy to Secure Cyberspace«, in which the President outlined his plan to »protect against the debilitating disruption of the operation of information systems for critical infrastructures and, thereby, help to protect the people, economy, and national security of the United States«.²⁴ In his remarks to the press following his nomination of Michael Chertoff as Secretary of Homeland Security on January 11, 2005, the President assured the country that, under Chertoff, the Department would continue in its primary mission, which he

described as »reduc(ing) the nation's vulnerabilities to weapons of mass destruction and cyberterrorism«. ²⁵

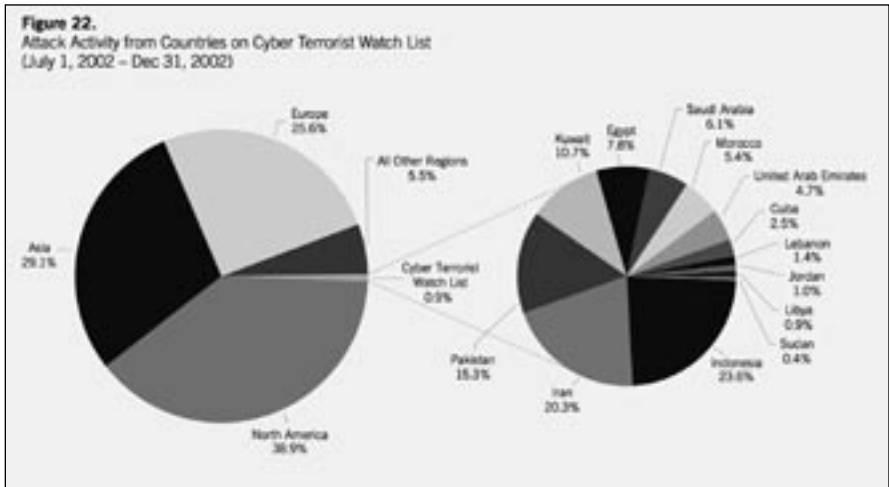
More recently, on June 9, 2005, during the President Bush's address to the Ohio State Highway Patrol Academy in which he urged the passage of the revised U.S. Patriot Act, the President argued that one of the primary reasons for the necessary expansions of powers under the new security act is to »renew the critical provisions of the Patriot Act that updated the law to meet high-tech threats like computer espionage and cyberterrorism«. ²⁶ In fact, in nearly every public discussion of the U.S. War on Terror since 9/11, the President has conflated the risk of conventional terrorist attacks with the risk of cyberterrorism, despite the fact, as »The National Strategy to Secure Cyberspace« admits, »the required technical sophistication to carry out such an attack is high – and partially explains the lack of a debilitating attack to date«. ²⁷ As their only illustrations of the otherwise unsupported statement that »the technical capability and sophistication of users bent on causing havoc or disruption is improving«, the document cited the 2001 Code Red and Nimda computer virus outbreaks, neither of which had previously ever been considered an incidence of cyberterrorism.

Similarly, private Internet security companies have never managed to demonstrate the threat of cyberterrorism, even though it might be in their direct financial interest to do so. In its semi-annual threat report of online security attacks for the third and fourth quarters of 2002, Symantec, the world's largest computer security corporation, included a special section on »Cyber-terrorism«. However, according to the report,

Countries on the (U.S.) Cyber Terrorist Watch List produced no severe events against companies in the sample set (...) Furthermore, Symantec detected no verifiable cases of cyber terrorist attacks during the past six months (...) Countries on the Cyber Terrorist Watch List generated less than 1% of all attacks detected during the past six months. ²⁸

Similarly, a more recent April 24, 2003, report by Peter Rojas of *The Guardian* stated that »according to Tim Madden, a spokesman for Joint Task Force – Computer Network Operations (JTF-CNO), created by the U.S. Strategic Command to handle network defence and attack, there has been no significant increase in attempts to infiltrate US military computers since the (Iraq, C.A.) war began«. ²⁹

More strongly, in the March 14, 2003, issue of *PC World*, Joris Evers reported on the results of an international cyberterrorism panel at the CeBIT technology trade show in Hanover, Germany. Consisting of executives from a number of leading international security software vendors, such as Counterpane Internet Security, RSA Se-



Symantec graph of attack activity from countries on the Cyber Terrorist Watch List during the period from 1 July 2002 to 31 December 2002. Source: Symantec Corporation, »Symantec Internet Security Threat Report: Attack Trends for Q3 and Q4 2002,« February 2003, 25. Available online at http://ses.symantec.com/PDF/Threat_Report_Final_4C.pdf.

curity, and Trend Micro as well as security representatives from the European Union and North Atlantic Treaty Organization (NATO), the panel unanimously concluded that »the cyberterrorism threat is overstated (...) and blame(d) the U.S. government, certain IT vendors, and the media for creating cyberterrorism angst.«³⁰ According to Rainer Fahs, Senior Information Security Engineer of NATO's Air Command & Control Systems Management Agency, »we do not see a terrorist attack on the Internet happening (...) Critical systems don't run on the Internet, they are based on secure networks, we have protected our systems and do not rely on the Internet.« Panelist Arthur Coviello, President and Chief Executive Officer of RSA Security, expressed his opinion that »the U.S. government after September 11 wanted a broader front to attack terrorism and cyberterrorism is part of that«.

However, few accounts have so comprehensively dismantled the Bush administration's post-9/11 obsession with cyberterrorism as *Washington Monthly* editor Joshua Green's »The Myth of Cyberterrorism«, which appeared in the November 2002 issue of the magazine.³¹ In the article, Green interviewed a wide range of military, governmental, academic, and private security experts in an attempt to ascertain the possibility of a cyberterrorist threat. With regard to the protection of defense and government-related information systems, Green found that in every area of critical U.S. infrastructure, including the entire defense and military weapons systems, the FAA's administrative and air traffic control systems, the CIA, the FBI, the INS,

NASA, and even the Department of Agriculture, the networks were overwhelmingly secure and most have even been »air-gapped«, or physically removed from Internet, for decades. When Green queried a retired military official as to the possibility of cyberterrorists accessing the U.S. governments nuclear weapons system via the Internet, Green observed that the official »was somewhat indignant at the mere suggestion«, replying »as a general principle, we've been looking at this thing for 20 years. What cave have you been living in if you haven't considered this [threat, C.A.]?«

With respect to non-governmental, »less-protected secondary targets«, such as »power grids, oil pipelines, dams, and water systems«, Green encountered similar responses. While many experts believe that a highly trained terrorist could conceivably hack into such secondary targets, »once inside, it would be far more difficult for him to cause significant damage than most people realize«. As Martin Libicki, a defense analyst at the RAND Corporation explained, »it's not the difficulty of doing it (...) It's the difficulty of doing it and having any real consequence.« Green also cited George Smith in regards to such vulnerabilities, who quipped that »no one explains precisely the hows, whys, and wherefores of these apocalyptic scenarios (...) You always just get the assumption that chemical plants can be made to explode, that the water supply can be polluted – things that are even hard to do physically are suddenly assumed to be elementary because of the prominence of the Internet.«

Green's investigative findings are corroborated by a December 2002 study for the United States Center for Strategic & International Studies by James A. Lewis, a 16-year veteran of the U.S. State and Commerce Departments. In examining the proposed vulnerabilities of multiple sectors of the United States critical infrastructure, Lewis concluded that in every region of analysis, including the water supply, power plants, power distributions networks, air traffic control systems, 9/11 emergency response systems, critical manufacturing industries, and military resources, »a closer look at the relationship between computer networks and critical infrastructures, their vulnerability to attack, and the effect on national security, suggests that the assumption of vulnerability is wrong«. ³² Notably, in regard to the possible disruption of the U.S. power grid, Lewis commented that »California's experience with »deregulation« in 2001, which resulted in »months of blackouts and rolling brown-outs«, was »a more powerful »attack« on the electrical infrastructure than anything a cyber-terrorist could mount«. ³³

Nevertheless, according to several measures of public opinion, the Bush administration's cyberterrorism campaign has been remarkably successful in alarming the American populace. In »The Myth of Cyberterrorism«, Green alludes to rather startling statistics regarding a National League of Cities survey of 725 city officials, which assessed the leaders' primary concerns for Homeland Security. The study,

entitled »Homeland Security and America's Cities«, which polled the municipal leaders between July and August of 2002, found that »among concerns about terrorist attacks, the possibility of biological, chemical, or cyber attacks ranks highest among city officials. More than four in five city officials said they were concerned or very concerned about biological (82%), chemical (81%), or cyber (80%) attacks«. ³⁴ Ironically, none of these three top-ranked means of attack have ever actually been deployed by foreign or domestic terrorists against the United States, whereas fears of much more probable methods of attack were reported as significantly lower, »including the possibility of a car or truck bomb (70%) or suicide bomb (62%)«. Even more surprising, given the fact that the survey was conducted after the 9/11 attacks, »the possibility of an airplane being used as a bomb or a missile ranked near the bottom of these concerns (60%) but was still cited by a majority of cities«. Fears about biological, chemical, and cyber terrorist strikes ranked even higher among cities with populations greater than 100.000 people, in which »threats of biological (95%), chemical (92%), and cyber (91%) attacks again rate as the three possibilities of greatest concerns«. More recently, a poll conducted in August 2003 by the Pew Foundation Project on the Internet & American Life and *Federal Computer Week* magazine found that half (49%) of 1.001 U.S. adults surveyed »fear that terrorists might cripple American utilities such as electric, transportation and water systems, or its banks and major corporations through cyber-attacks«. ³⁵

The Benefits of Bad Information

While it is difficult to deny that computer viruses and other malicious Internet attacks do pose some ill-defined risk to American security and economic interests, this threat is radically disproportionate to the stunning degree of rhetorical posturing the Bush administration has mobilized around the topic. In attempting to understand the Administration's rationale for so aggressively pushing its cyberterrorism agenda, Green arrives at two likely explanations: it is a means for revitalizing a sluggish economy and for distracting from its other political activities. With regards to his first postulate, Green quotes Ohio State University law professor Peter Swire's observation that »many companies that rode the dot-com boom need to find big new sources of income. One is direct sales to the federal government; another is federal mandates. If we have a big federal push for new security spending, that could prop up the sagging market.« Green elaborated on his second reason for the over-hyping of cyberterrorist threats with the comment that »stoking fears of cyberterrorism helps maintain the level of public anxiety about terrorism generally, which in turn makes it easier for the administration to pass its agenda«.

In many ways, the war on cyberterrorism has become the most seductive component of the President's larger War on Terror in that it actively enlists all patriotic Americans to serve in the effort. »The National Strategy to Secure Cyberspace« splits its »problem« of »threat and vulnerability« into five different levels: (1) the Home User/Small Business, (2) Large Enterprises, (3) Critical Sectors/Infrastructures, (4) National Issues and Vulnerabilities, and (5) Global.³⁶ Within such a hierarchy, the »increasing awareness about cybersecurity« among home and small business users is of vital importance, considering that »home users and small business owners of cyber systems often start with the greatest knowledge gap about cybersecurity.«³⁷ In fact, the issue of home user cybersecurity is of such importance to the defense of the Nation that its responsibility must not be limited only to adults. With this in mind, the Department of Homeland Security has pledged to »partner with the Department of Education and state and local governments to elevate the exposure of cybersecurity issues in primary and secondary schools.«³⁸ As Sarah D. Scalet warned in the title of her October 11, 2001, edition of her biweekly column on computer security, »cyberterrorism is Everyone's War.«³⁹ Thus, cybersecurity has become the War on Terror's equivalent to the Cold War proscription that every American family constructs a nuclear fallout shelter in its backyard. Thanks to cybersecurity, the War on Terror has become a war that we can all actively engage in from the comfort of our own homes.

From an expanded perspective, the Bush administration's seemingly unjustifiable »war« on computer viruses and cyberterrorism is completely consistent with its larger crusade against all things ontologically challenging, including cloning, stem cell research, abortion, and same-sex marriage. Even more so than President Nixon's War on Cancer of over thirty years ago, these more recent battles prey on Americans' numerous fears of the unfamiliar, the uncontrollable, and the uncertain. They are all intangible »moral« struggles, which inspire jingoistic rhetoric without any possibility for accountability, particularly in the case of computer viruses since there currently is no reliable procedure by which to measure relative success or failure. Not that ability to ascertain progress matters. As long as new computer viruses occasionally get released on the Internet (as they inevitably will) and regardless of whether they originate from a terrorist source (as they most likely will not), the Administration will point to them as evidence of the continued need for the larger War on Terror. Whenever there is a lull in online attacks, the Administration can tout the effectiveness of their current security solutions. Either way, the political result is the same. No other outcome is possible, as they have sealed the issue within a completely closed, infinitely replicating, binary loop – one that is completely identical to the kind of inescapable logical trap a virus would use to bring down a computer system.

Notes

- 1 John Leyden, Lies, Damned Lies and Anti-Virus Statistics, in: *The Register* (18 January 2002); available online at http://www.theregister.co.uk/2002/01/16/lies_damned_lies_and_antivirus.
- 2 Ibid.
- 3 Eric Goetz, Guofei Jiang and William Sterns, Viruses and Worms, in: *Investigative Research for Infrastructure Assurance Group* (Institute for Security Technology Studies, Dartmouth College, March 2002), 12; available online at <http://www.ists.dartmouth.edu/analysis/vw0302.pdf>.
- 4 Ibid, 13.
- 5 Ibid.
- 6 CERT/CC Statistics 1988-2005; available online at http://www.cert.org/stats/cert_stats.html#incidents.
- 7 Available online at <http://sun.soci.niu.edu/~crypt>.
- 8 George Smith, An Electronic Pearl Harbor? Not Likely, in: *Issues in Science and Technology* (Fall 1998); available online at <http://www.issues.org/issues/15.1/smith.htm>
- 9 Ibid. For a more recent example of the »electronic Pearl Harbor« scenario, see Dickon Ross, Electronic Pearl Harbor, in: *The Guardian* (20 February 2003); available online at <http://www.guardian.co.uk/online/story/0,3605,898662,00.html>.
- 10 The main technical difference between viruses and worms is that viruses infect and spread themselves by means of another »host« application, whereas worms contains its own means for replication and can spread itself to other computers without a host.
- 11 For a discussion of epidemiological and immunological models of computer viruses, see the following: Cliff Changchun Zou, Weibo Gong and Don Towsley, Code Red Worm Propagation Modeling and Analysis, in: *Proceedings of the 9th ACM Conference on Computer and Communications Security* (November 28-22, 2002), 138-147; Stephanie Forrest, Steven A. Hofmeyr and Anil Somayaji, Computer Immunology, in: *Communications of the ACM* 40 (October 1997), No. 10, 88-96; Harold Thimbleby, Stuart Anderson and Paul Cairn, A Framework for Modelling Trojans and Computer Virus Infection, in: *Computer Journal* 41 (1999), No. 7, 444-458; and Jeffrey O. Kephart and Steve R. White, Directed-Graph Epidemiological Models of Computer Viruses, in: *IEEE* (August 1991), 343-359.
- 12 Robert Ausch, Randal Doane and Laura Perez, Interview with Elizabeth Grosz, *Found Object* (9), 1-16. <http://web.gc.cuny.edu/csctw/found%5Fobject/text/grosz.htm>
- 13 Jussi Parikka, Digital Monsters, Binary Aliens – Computer Viruses, Capitalism and the Flow of Information, in: *fibreculture* (4) 2005, http://journal.fibreculture.org/issue4/issue4_parikka.html.
- 14 Alan F. Kay, The Lessons of Y2K – 1st Global Technological Meltdown Averted ~#44, in: *The Polling Critic* (10 January 2005); located online at <http://www.cdi.org/polling/44-y2k.cfm>.
- 15 Located online at <http://www.sec.gov/rules/interp/33-7558.htm>. For complete coverage of the SEC activities with respect to Y2K compliance, see <http://www.sec.gov/news/extra/y2k/home2000.htm>.
- 16 Associated Press, SEC sets deadline for Y2K compliance, in: *JSONline* (27 July 1999); located online at <http://www.jsonline.com/bym/tech/news/jul99/y2k-brokerages072799.asp>. SEC document located online at <http://www.sec.gov/rules/final/34-41661.htm>.
- 17 George Smith, Electronic Pearl Harbor. A Slogan for U.S. Info-Warriors, in: *The Crypt Newsletter*; located online at <http://www.soci.niu.edu/~crypt/other/harbor.htm>.
- 18 For an example of Clarke's use of the term, see Tim Weiner, The Man Who Protects America From Terrorism, in: *The New York Times* (1 February 1999), A3.
- 19 Philip Buckley, Information Security, New Niche, in: *SecurityDocs.com Security White Papers and Articles* (12 October 2004); located online at <http://www.securitydocs.com/library/2639>.
- 20 Eliza Williams, Climate of Fear, in: *Forbes.com* (4 February 2002); available online at <http://www.forbes.com/forbes/2002/0204/064.html>.
- 21 Office of the White House Press Secretary, Fact Sheet on New Counter-Terrorism and Cyber-Space Positions (9 October 2001); available online at <http://www.whitehouse.gov/news/releases/2001/10/20011009.html>.
- 22 US Presidential Executive Order on Critical Infrastructure (16 October 2001); available online at <http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html>.

- 23 Transcript from the Office of the White House Press Secretary, President Bush Signs Homeland Security Act (25 November 2002); available online at <http://www.whitehouse.gov/news/releases/2002/11/20021125-6.html>.
- 24 George W. Bush, The National Strategy to Secure Cyberspace (February 2003); available online at http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.
- 25 Transcript from the Office of the White House Press Secretary, President Nominates Michael Chertoff as Secretary of Homeland Security (11 January 2005); available online at <http://www.whitehouse.gov/news/releases/2005/01/20050111-2.html>.
- 26 Transcript from the Office of the White House Press Secretary, President Discusses Patriot Act (9 June 2005); available online at <http://www.whitehouse.gov/news/releases/2005/06/20050609-2.html>.
- 27 The National Strategy, as note 24.
- 28 Symantec Corporation, Symantec Internet Security Threat Report.. Attack Trends for Q3 and Q4 2002 (February 2003), 24; available online at http://ses.symantec.com/PDF/Threat_Report_Final_4C.pdf.
- 29 Peter Rojas, The Paranoia that Paid Off, in: The Guardian (24 April 2003); available online at <http://www.guardian.co.uk/online/security/story/0,14230,1145061,00.html>.
- 30 Joris Evers, Does Cyberterrorism Pose a True Threat?, in: PC World (14 March 2003); available online at <http://www.pcworld.com/news/article/0,aid,109819,00.asp>.
- 31 Joshua Green, The Myth of Cyberterrorism, in: Washington Monthly (November 2002); available online at <http://www.washingtonmonthly.com/features/2001/0211.green.html>.
- 32 James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats (December 2002), 1; available online at http://www.csis.org/tech/0211_lewis.pdf.
- 33 Ibid, 5.
- 34 Christopher Hoene, Mark Baldassare and Christiana Brenna, Research Brief on America's Cities. Homeland Security and America's Cities, in: Issue (December 2002), No. 2; available online at <http://www.nlc.org/content/Files/RMPHomelandsecbrf02.pdf>.
- 35 Lee Rainie, Pew Internet Project Data Memo. Survey with Federal Computer Week Magazine about Emergencies and the Internet (31 August 2003); available online at http://www.pewinternet.org/pdfs/PIP_Preparedness_Net_Memo.pdf.
- 36 The National Strategy, as footnote 24, 7-8.
- 37 Ibid, 38.
- 38 Ibid, 39.
- 39 Sarah D. Scalet, Cyberterrorism Is Everyone's War, in: CSO (11 October 2001); available online at <http://www.csoonline.com/alarmed/10112001.html>.