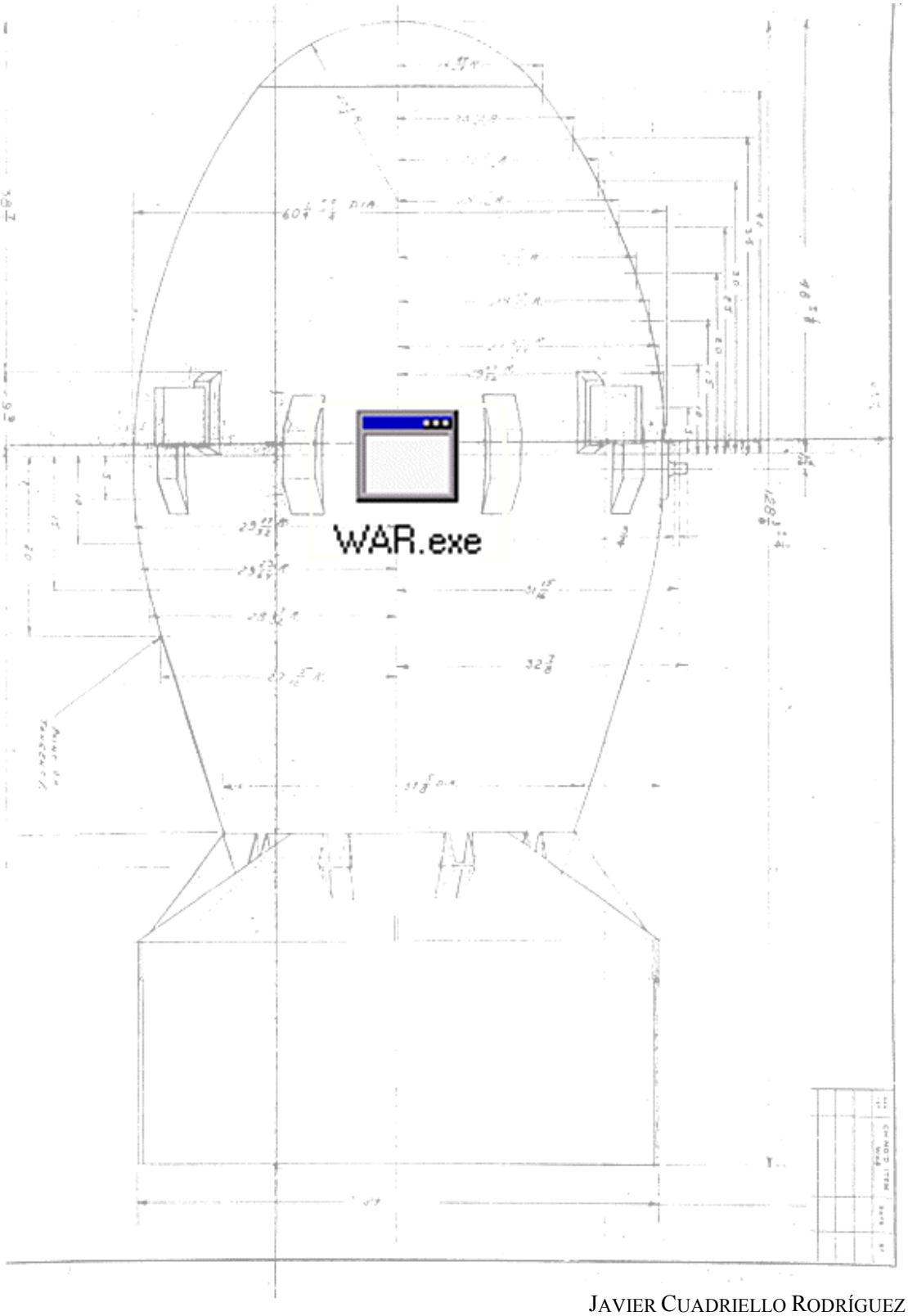


JAVIER CUADRIELLO RODRÍGUEZ
LONDON SCHOOL OF ECONOMICS
DEPARTMENT OF INFORMATION SYSTEMS
London, April 2001

WAR.exe - One step ahead or one step behind

On the morning of the 31st of July, 1588, the Spanish Armada proceeded cautiously up the English Channel in battle formation. An English pinnace, the *Disdain*, fired a single shot towards the Spanish ships. In this fashion, the challenge of Lord Admiral Howard of Effingham was carried to the Duke of Medina Sidonia, commander of the Armada.[1]

Soon after, the English fleet approached in a formation never before experienced in battle, sailing in a single line. The new tactics which Lord Howard's fleet was going to employ throughout the campaign were now revealed. As the long file of vessels approached, each in turn fired a broadside before heeling away beyond range of the Spanish guns, only to circle and repeat the process again. There was to be no mass attack, and the hand-to-had combat the Spaniards had expected. Something entirely original was occurring.[2]

The development of naval warfare had received scant attention from Spain's professional militarists, many of whom continued to regard the ship as little more than a floating battlefield where soldiers stood and fought, and the use of heavy guns as a distinctly unchivalrous form of combat. These ideas were seen by the English as totally outdated – the development of the long-range gun had signalled the end of that concept. Having, unlike the Spaniards, rejected the long established idea that naval warfare consisted of grappling and boarding, England's ship designers concentrated on a new generation of faster and more manoeuvrable vessels. The potential of the long-range gun had been recognised by English strategists to a far greater extent than it had by the Spaniards and although in the run-up to the campaign, the Spanish had made strenuous attempts to increase their supply of long-range guns, their efforts had been thoroughly belated. [3]

As in the case of the English long range cannons or the iron sword, gun powder and many others before; new technologies allowed new possibilities and tactics. As Bernard Brodie, the famous North American. military strategist, put it referring to the effect of airpower on war, "The airplane appears, and a …new military philosophy [is] centered upon it. Then nuclear weapons and rocket vehicles come along, and these create wholly new conditions… including certainly possibilities of unprecedented war. "[4]

History has shown in several occasions that, as Spain did with the Armada, countries are often trained and equipped for the last war. Large sums of money and resources can be used to purchase or develop the wrong weapons for the wrong kind of war. Is there then something that can be learnt from History?

For most of the second half of the 20th century, industrialised nations entered an arms race preparing for a nuclear war that luckily never materialised. The political scenario changed with the fall or the Soviet Union. Instead of the expected nuclear conflict, the world has seen a combination of guerrilla wars in the third world and usually US/NATO lead hi-tech post-modern wars.

The industrialised world is now struggling to adapt its armed forces to reflect this new situation and acquiring and developing new and expensive weapons such as US$28m (projected price) Joint Strike Fighters (JSF) and Laser and GPS* guided 'smart' bombs. They are also adapting other weapon systems designed for a nuclear war, such as the US$2.4b B-2 bombers for different types of conflicts. But is this what the next war is really going to be about or is it just a preparation for another Gulf war that may never happen again?

Lockheed Martin proposed JSF for the U.K. Royal Navy. Artist conception. [5]

6

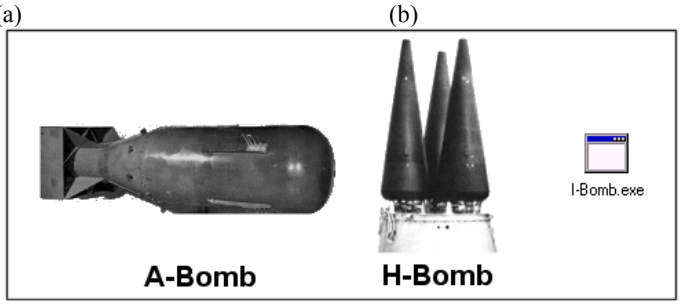
Laser Guided Bomb (GBU-28)

THE NEW INFORMATION SOCIETY

Long after the Armada battles and the after the Cold War we have arrived to the long awaited new millennium. Technology has not developed 'cool' flying cars and generalised space travel but it has infiltrated in a much more subtle way, almost in a viral fashion, every part of human activity. Today the world is virtually controlled by computers; the economic system, water, electricity, gas, voice and data communications, rail and air traffic control, government and the military are completely dependent on computers. Everyday this tendency increases and we do not have old fashion systems as backup available.

It seems reasonable then, that in a hypothetic future war, targeting enemy computer systems will be a priority and, more than ever, technology will be used to fight technology. Paradoxically, the Internet was developed to resist a nuclear war, but for every new defence there is a new weapon and vice-versa. There could be potentially catastrophic consequences for a cyber attack and analogies such as the Electronic Pear Harbor and the Information Bomb therefore come to mind.

(a) (b)



7

(a) Little Boy (first nuclear bomb used in Hiroshima)
(b) Intercontinental Ballistic Missile (ICBM)
W-78 warhead (Fission bomb)

* Global Positioning System

VULNERABILITY OF THE INFORMATION SOCIETY

In 1994 a team of in-house hackers was unleashed by the U.S. Defence Information Systems Agency on military computers and penetrated 88% of the nearly 9,000 attacked. Only 4% of the penetrations were even noticed. More recently, 155 federal computers systems some with sensitive research information were taken over by hackers last year and 32 North American federal agencies were struck by foreign attackers.[8]

Robal L. Dick, director of the FBI National Infrastructure Protection Center (NIPC) has said that, as of April 2001, there are 102 open investigations of computer intrusions into U.S. government systems and that the bureau is aware of a rise in alleged state-sponsored hacking. On the other side of the Atlantic, British Foreign Secretary Robin Cook has warned that computer hacking may pose a greater threat to the national infrastructure than a conventional military attack[9].

We must also remember that the vulnerability of many information systems may not even be a purely technological one. Kevin Mitnick, famous for his penetration of several government and corporate computer systems,[10] admitted that most of his hacks consisted of so called 'social hacks'. This kind of hack involved convincing employees that, for example, he worked in the IT department of the company and that he could be trusted. This allowed him to obtain information that he could use to gain access to the company's computer systems. As Mitnick told the members of the U.S. Senate Committee on Governmental Affairs, "The weakest link in the security chain is the human element."

An added problem is the difficultly of distinguishing an attack from an accident or technical breakdown. This was already the case on the 19th of May 1998, synchronizing almost perfectly with the Birmingham summit of the G8, when the Galaxy IV telecommunications satellite suddenly interrupted the messages of some 90% of the USA's 45 million pagers for nearly a day after the on-board computer had slightly shifted the satellite's position[11-12]. If electronic attackers are good enough to cover their tracks, the possibility of a retaliatory response would be seriously hampered as the victim would not know if there had been attack and where to retaliate. As Sun Tzu's Art of War written around 2500 year ago explains, "You can ensure the safety of your defence if you only hold positions that cannot be attacked"[13], and this is precisely the position where a good hacker would be.

The Galaxy satellite incident provides a good example of the dependency of civilian communications on technology and the consequences of single point failures in some of the current information infrastructure. Military forces also rely extensively in space, especially for intelligence gathering and communications. According to U.S. Space Command, the United States has slightly more than 300 active satellites. Of those, 60% are commercial, 20% are military and 20% belong to civilian government agencies.[14]

Disabling some satellites by hacking into their control centres, rather that using expensive anti-satellite missiles that few countries can afford, could blind the military and make a potential conventional attack possible. For example, troops could be moved without the party trusting its

intelligence satellites knowing. Also, disabling radar tracking stations could render the multi-billion dollar proposed American National Missile Defence (NMD) inoperative. Thus, not only could a cyber attack create an electronic Pearl Harbor, but it could also make an old fashion one possible.

These weaknesses are compounded by the fact that military and civilian information systems are intimately linked. Railroads for example, are controlled by relatively penetrable civilian systems and much of the military's unclassified message traffic travels on the Internet. According to *The Washington Post* over 95% of U.S. military communications go over civilian networks and there are at least 150,000 military computers connected directly to the Internet. In cyberwar, civilian information systems can be as critical as military systems and any effort to build a truly secure national information systems will require close cooperation between businesses and governments[15]. In this way, everybody, not just the military, should be ready for war, making war, to some extent, part of the civilian life as defended by Machiavelli in his 1521 book *The Art of War.*[16]

The cyber attacks that have happened until now have only been relatively small-scale criminal acts. However if the current systems are vulnerable to these crimes, they will be even more vulnerable in a war situation, which could be seen as nothing else than a big 'legitimate' crime carried out by better equipped people. If amateur hackers with simple programs can cause some economic damage to *Yahoo!* and *Amazon* why wouldn't elite programmers hired and/or trained by the military be able to produce far greater damage?. Criminal acts may actually act as a short of vaccine and create an awareness that will make companies and countries protect themselves against, at least, the most simple forms of attack. But in the same way that locking your door may stop some burglars but not an enemy soldier, these measures may be insufficient in the event of a cyberwar.

LARGE SCALE, NATION VS. NATION WAR AND GUERRILLA WARFARE

Nation vs. Nation

> *"Can we say that in today's [wars] man is pitting his strength, skill, courage, or endurance against man? Certainly not! War has become a contest between machines, industrial enterprise, and financial organizations."*
>
> - Bronislaw Malinowski, Address, Harvard, September 1936.[17]

A large scale war between nations can be seen as a form of very aggressive economic war. Whichever nation can provide more economic, industrial and human resources to maintain the war effort is, in theory, likely to win. In a hypothetical cyberwar with an assumed small or null loss of human life, the relevance of the idea of economy vs. economy becomes ever clearer.

As with all new military technologies, like the long range English cannons and fast vessels, the most advanced nations in cyber attack/defence technology will gain the upper-hand over their enemies. In this way, information technology will become the ultimate weapon for economic wars, being used in both the business world and the battlefield to gain competitive advantage over adversaries.

On the other hand, a highly developed country which is largely dependant on its information infrastructure but that is not ready to defend against an electronic attack, becomes a far more vulnerable target in this kind of warfare than an undeveloped country.

Then, in theory at least, a cyber attack could limit the military's capacity to provide a conventional response and then attack the electronic communications dependent economic activity directly. This promises to make cyberwars shorter and more efficient, saving the long process of exhausting the adversary's resources through months or years of combat. That is, the efficiency of information technology, often associated with electronic commerce, also applied to war.

At the same time, however, the boundaries of an open war could become less clear, and country could try to sabotage another country's economy without openly declaring war or ever admitting any kind of attack. It opens a possibility for new temperature gradients in war, from cold to hot and warm wars with continuous and silent sabotage of enemy infrastructure and also new forms of economic sanctions which could openly declared or not.

Guerrilla warfare

In theory, a cyber attack requires a small capital investment to achieve tremendous results compared with conventional weapon systems, which makes it ideal for guerrilla warfare.

We already have some limited examples of this guerrilla cyberwar. The so called 'e-Jihad' or 'inter-fada' and the Israeli equivalent, has for the moment been limited to defacing websites by placing slogans and flags from the opposite side; not really hacking but only 'net cracking'. However, the sophistication of attacks is expected to increase as attackers on both sides have time to prepare and lay out more intricate actions[18]. For example, an attack on the Israeli Defence Force (IDF) intelligence could be used to plan attacks and avoid retaliatory responses. Furthermore, stealing trade secrets form Intel's plants in Israel or attacking American Jewish banks could internationalise the conflict.

Cyberwarfare may not necessarily depend on multi-bi/million dollar weaponry as more damage could be caused more cheaply by small viruses and cracking systems created by a small team of talented hackers. This team of computer mercenaries, a proto-version of those depicted in Gibson's near-future universe in *Neuromancer*[19], could be hired for less than the cost of one fighter aircraft[20]. This relatively small cost could also blur borders between conventional and guerrilla warfare. The balance of power could shift or at least spread more evenly among the nations, but also terrorist organizations and organized crime. In the same way the British –considered by the Spaniards and the Catholic Church as a 'rogue' state at the time- could not accept to surrender to the Armada, some states and ideological groups may not be willing to accept the US/NATO military hegemony. Cyberwar brings the perfect opportunity for action for these so called 'rogue 'states – defined today

as those which oppose U.S. interests specifically and global security more broadly[21]–, former superpowers and fundamentalist groups.

THE NEW HERO AND THE NEW VILLAIN

In a cyberwar a single champion, a single computer genius, could be the most powerful weapon in a country's arsenal. This individual could be born anywhere and be loyal to any ideals, including money, like as the mercenary 'jockeys' (a kind of professional network hackers) in Gibson's universe.

The new stereotype of enemy and war hero may move respectively from the SS soldier or the KGB agent and U.S. Marines holding oversized flags over Iwo Jima for example, to the Russian or Islamic fundamentalist computer nerd. Looking at James Bond movies for an example of society's views about 'the enemy', we can see how this change is to some extent already happening. From the old villains stealing nuclear warheads from the 60s to the 80s in *ThunderBall* (1965), *Octopussy* (1983) and others, to the new villains controlling electromagnetic pulse weapons to stop computer systems in *Golden Eye* (1995) or controlling the media, another form of information (or disinformation) warfare, in *Tomorrow never dies* (1997). Eventually cyberwar with its relative cleanliness could not compete with the much more dramatic and Hollywood-like idea of a nuclear explosion, which regained the central role in *The world is not enough* (1999).

THE CONTRAST

THE NERD

"*Yes! I am invincible!"*
- Boris Grishenko in GoldenEye

THE OLD HERO

The Iwo Jima Memorial

"*Among the Americans who served on Iwo Jima, uncommon valor was a common virtue."*
- Admiral Nimitz

POLITICALLY CORRECT (CYBER)WAR

"American policy is to expend machines rather than men"
- Intelligence officer, 20th Airforce [22]

According to Chris H. Gray, Associate Professor Cultural Studies of Science, Technology and Computer Science of the University of Great Falls, in his book *Post-modern War*, "the central role of human bodies in war in being eclipsed rhetorically by the growing importance of machines in general and weapons in particular. The number of Iraqi tanks and planes destroyed was always available; the count of dead Iraqi bodies was not. It was considered as a 'distasteful' or 'pornographic' interest by one British briefing officer."[23]

Getting killed and even killing is increasingly being considered as unacceptable even in war. As Gray points out in his book, General H. Norman Schwarzkopf even went so far as to say that "we are

not in the business of killing"[24]. These ideas come mainly from the North American politically correctness culture, which extends into the whole industrialized world.

Today, B-52 and B-2 bomber crews fly from the U.S. to attack remote parts of the world and come back home for dinner. It seems that we are trying to achieve an ultimately convenient and clean war. As summarised in the 1948 book *The Science of War*[25], "The romantic conception of war is becoming out of date. It is not consonant with the systematic, rational, scientific kind of warfare which is evolving from the inter-penetration of war and science… For the traditional romanticism of war is the contrary of the civilian scientific spirit." The honour and the glory once associated with a fair close combat, as already shown for by the English Navy against the Armada and the stealth NATO bombers over Iraq and the former Yugoslavia, are romantic notions made obsolete by science and technology.

However, despite the refusal of the western world countries to shed blood in war, they do not seem to be willing to give up on wars either. This applies to the US in particular which, as put by Brigadier General William 'Billy' Mitchell, "[America] is one of the most warlike nations on Earth."[26] There is a point where not even politically correctness can defeat the violent impulses of human nature. As already accepted in the writings of the 18th century Prussian military thinker Carl von Clausewitz, the existence of political violence is inevitable, and as summarised in his famous sentence, "War is merely a continuation of politics" - or "of policy" depending on the translation of the original *Politik* in German.

Then, as the armies of the industrialised world are forced to avoid the risk of any casualties, the promises of bloodless cyberwar become more seductive.[27] In theory, a cyberwar would allow a 'limited war'. Nations try to put limits on war; explosive bullets were already forbidden in the St . Petersburg Declaration in 1868[28], the 1968 Treaty on the Non-Proliferation of Nuclear Weapons, (NPT), the destruction of antipersonnel mines and chemical and biological weapons are examples of this.

Cyberwars promise the ultimate way of surgically attacking only the strategic targets leaving innocent civilians untouched with a lower cost and risk of failure and collateral damage than a Tomahawk missile. Continuing with the conventional weapons analogy, the I-bomb is 'sold' as the ultimate smart bomb rather than the ultimate nuclear bomb.

However, surgical attacks may not be as trivial as predicted, as would be avoiding innocent civilian suffering. It is true that human blood would not be spilled by the military, but its consequences may cause economic instability and chaos that could leave millions in a precarious economic situation. Furthermore, the increase in the globalisation of commerce and the aim of global free trade, along with the fact that technology is what largely makes this internationalisation of commerce possible; is strongly linking the destiny of the different nations. Therefore and despite of some nationalistic views, there are no longer nations of a special, 'universal destiny'. A form of war that can reach the core of the economy of a key trading country could have important implications for its trading partners. As the most obvious example, paralysing, or even

worst, feeding false information into the NYSE's computer systems would have an unpredictable effect on the world's economy. Therefore, a large scale attack on the economic infrastructure of a country could quickly escalate into some form of a world war, possibly into a conventional war.

DEFENCE EFFORTS AGAINST CYBERWAR

> *"It is probable that future war will be conducted by a special class, the air force, as it was by the armored Knights of the Middle Ages."*
>
> - Brigadier General William 'Billy' Mitchell, 1924.

The United States geographic location has placed it outside the reach of most threats to its internal critical infrastructure. Cyberwar, for the first time since the Intercontinental Ballistic Missile (ICBM), threatens this. The U.S. government has taken the lead in developing systems to protect their information infrastructure against a possible cyber attack and to create a retaliatory electronic response. Although a 5th force to be added to the Air force, Navy, Army and Marines has not (yet?) been proposed, several groups depending on several agencies have been created for this task, operating not without certain responsibility conflicts between them.

In 1995 the U.S. formed the interagency Critical Infrastructure Working Group (CIWG) to review critical internal infrastructure vulnerability to terrorism including the possibility of cyber attacks. Responding to the CIWG recommendations, the President's Commission on Critical Infrastructure Protection (PCCIP) was created to report to the President on threats involving vulnerabilities to critical national infrastructures, while providing policy alternatives and solutions.[29]

The Federal Bureau of Investigation (FBI) through the National Infrastructure Protection Center (NIPC) serves as an early warning centre for information system attacks. The FBI also operates the highly publicised Carnivore system for electronic wiretapping. The U.S. Department of Defense (DoD) and other military agencies also play key roles in protecting sensitive information and infrastructure. Much of the responsibility for dealing with cyber threat and response policies is consolidated under the Assistant Secretary of Defense C^4I (Command, Control, Communications, Computer & Intelligence).

Great part of the military defence systems are controlled by the U.S. Space Command. It controls the Joint Task Force – Computer Network Defense (JTF–CND) and the CNA (Computer Network Attack) which were designed to serve as the focal point for defence of DoD computer systems and their mission includes counter-terrorism and support of U.S. military forces deployed in crisis or conflict. In addition, some of the reserve forces, such as the Army Reserve, have created information operations centres trained and manned by so-called 'cyber-defence warriors'.[30]

However, the responsibility is clearly fragmented and in the same way that is it clear that the U.S. Navy defends the interests of the United States at sea, it is, at the moment, not as easy to explain who defends its interests in 'cyberspace'. Some consolidation of efforts and resources for the protection of the information infrastructure is required, and is slowly starting to appear.

The National Plan for Information System Protection (NPISP), Version 1.0 [31], created in January 2000, was the first attempt of the U.S. Government to develop a comprehensive plan to defend its cyberspace. The first version of the National Plan focuses on the efforts being undertaken by the U.S. Federal Government to protect the critical cyber-based infrastructures. It includes the FidNet (Federal Intrusion Detection Network) system for monitoring non-military government computers, in an effort to protect them from hacker attacks. FidNet , as Carnivore, has raised some debate over its possible violation of the Fourth Amendment to the U.S. Constitution, which bans unreasonable searches and seizures. According to *The Industry Standard Magazine* (TheStandard), Critical Infrastructure Assurance Office (CIAO) director John Tritak dismissed the critics calling FIDNet nothing more than a "federal burglar alarm for civilian government computer systems."[32]

According to the CIAO, "subsequent versions of the National Plan (NPISP 2.0)[33] will incorporate a broader range of concerns, including the specific roles that industry, state and local governments will play in protecting privately owned infrastructures".[34]

The computer industry is already getting involved. In January 2001, The U.S. Commerce Department and executives from nineteen information technology companies including Microsoft, Oracle, Cisco, IBM, HP, EDS, Intel, Symantec and others, announced the formation of the Information Technology Information Sharing and Analysis Center (ISAC). The ISAC will share information about cyber attacks, protective measures, and other information security issues.[35]

There are some critics of these protection systems, drawing comparisons with the National Missile Defense (NMD). However an equivalent to the 1972 Anti-Ballistic Missile (ABM) between the United States and the Soviet Union seems impossible as in cyberwar, with its appealing characteristics for terrorist groups, it cannot be established who are the potential contenders who should sign such a treaty.

Other nations seem to be placing significantly less resources (if any) in this field. However, the U.S. protection system does not extent beyond its national borders. In the event of a full scale electronic attack and assuming that the defence systems worked as expected and were sufficient to maintain and the U.S. internal electronic infrastructure intact; they could still be affected by the collateral economic damage of a successful large scale attack on another country, an oil or technology supplier for example.

The question is whether or not these efforts will be enough to keep the United States, as their British ancestors in the battle against the Armada before them, one step ahead in their preparation for war. Or it will be, as the Spanish late acquisition of long range guns, one step behind terrorist groups and 'rogue' states. Finally, it remains to be proven if all these preparations for cyberwar are not just a reaction to the usual hysteria coming from the fear of new technologies and their over-hyped consequences.

On the cover page: *Fat man* (Atomic bomb dropped over Nagashaki) blue print and Microsoft Windows icon.

[1] Milne-Tyte, R. (1998). Armada! Hertfordshire, Wordsworth Military Library.

[2] Milne-Tyte, R. (1998). Armada! Hertfordshire, Wordsworth Military Library.

[3] Milne-Tyte, R. (1998). Armada! Hertfordshire, Wordsworth Military Library.

[4] Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press. P.130

[5] Images from the Federation of American Scientists (FAS)

[6] Image from the Federation of American Scientists (FAS)

[7] Image from the Federation of American Scientists (FAS)

[8] Associated Press (2001). Report: 155 federal systems hacked last year. Cnn.com.

[9] Knigh, W. (2001). One in three U.K. companies have been hacked. ZDNet(UK).

[10] Schwartz, J. (2000). Washington Post. Washington D.C.**:** p. E01.

[11] Virilio, P. (2000). The Information Bomb (Bombe informatique). London, Verso : p.141

[12] Stone, A. (2001). Dependence on satellites puts nation at risk. U.S.A. Today.

[13] Sun Tzu (about 500 B.C). The Art of War.Translated from the Chinese by Lionel Giles, M.A. (1910).

[14] Stone, A. (2001). Dependence on satellites puts nation at risk. U.S.A. Today.

[15] R. P. C. Americo (2001). Cyberwar: The mice is mightier than the missile, Military and C4I , from Infowar.com.

[16] Machiavelli, N. (1990). The Art of War, E. Farnsworth. as quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[17] As quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[18] R. P. C. Americo (2001). Cyberwar: The mice is mightier than the missile, Military and C4I , from Infowar.com.

[19] Gibson, W. (1984). Neuromancer. New York, Ace Books.

[20] R. P. C. Americo (2001). Cyberwar: The mice is mightier than the missile, Military and C4I, from Infowar.com.

[21] O'Sullivan, M. L. (2000). “Les dilemmes de la politique américaine vis-à-vis des 'Rogue'.” Politique Etrangère, Review of the French Institute of International Relations (IFRI), Paris.

[22] As quoted in Sherry, M. S. (1977). Preparing for the Next War: America Plans for Postwar Defense, 1941-45. New Haven, Conn, Yale University Press. As quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[23] Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[24] Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[25] J. Crowther and R.Whiddington, The Science of war, 1948, pp.119-120 as quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press., p.129.

[26] Brigadier General William 'Billy' Mitchell quoted in Flanklin, B. (1988). StarWars : he superweapon and American Imagination. Oxford, Oxford University Press**:** p.99. as quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[27] Sisk, R. (1995). In the Age of High Tech Cybergrunt, Old soldiers never lie. Oregonian**:** p. A7. and Black, C. (1994). U.S. options seen fewer as military avoids risk. Washington Post. Washington**:** p.A3. as quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.

[28] Michael Glover, The Velvet Glove: The decline and Fall of Moderation in War (1982, p15) as quoted in Gray, C. H. (1997). Postmodern war - The new politics of conflict. New York, Guilford Press.p.110

[29] Lacombe, P. and D. Keyes (2000). "Defending the American Homeland's Infrastructure."

[30] Hildreth, S. A. (2000). Cyberwarfare - Congressional Research Service (CRS) Report for Congress.

[31] The White House (2000). "National Plan for Information Systems Protection - Version 1.0."

[32] Perine. K. (2000) Senators, Privacy Advocates Spar Over FIDNet Plan. The Standard Industry Magazine.

[33] Littger. P. , The angst of the @-bomb. What is cyberwar? A status report.

[34] Critical Infrastructure Assurance Office (CIAO) (2001). Key Initiatives.

[35] Tech Law Journal (2001). "Commerce Dept. and 19 Companies Announce IT Security Group." Tech Law Journal.