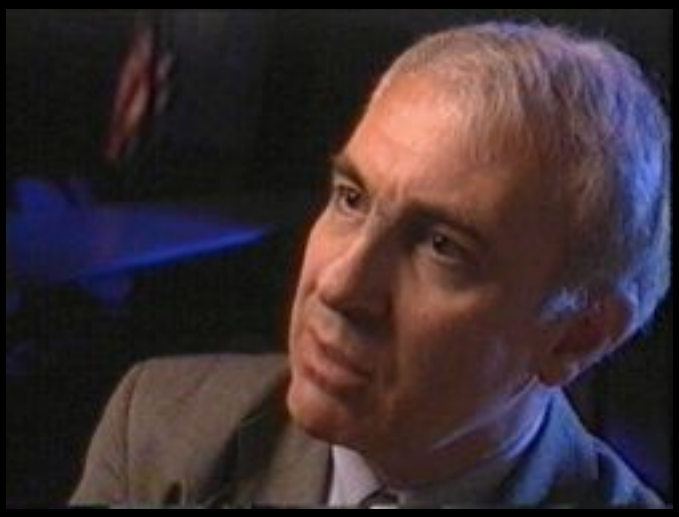
Title: SCRIPT: "CYBERWAR" PAGE ONE



DAN KUEHL
When I crossed your national boundary with an army and invaded your country - that was war. If I come in with a fleet of a hundred bombers and devastate your country with bombs that's obviously warfare, but in the information age - in the cyber-age what's the equivalent of that?..

NARRATOR (RALPH INESON)
Throughout history we've always known what war was about - physical attacks with swords, spears, bombs and bullets. But today that's changing.

DAN KUEHL
Joe Q citizen, can't go out and by an F1-17 or Tornado fighter plane or an attack submarine. But with a relatively simple computer capability as we have seen over and over again, individuals can do things via the cyberspace environment, that can impact on the national security interests of actual nation states.

NARRATOR
Military leaders brought up on missiles and nuclear deterrents are struggling to respond to an entirely new threat. The launch pad no longer a runway, but a computer - the attacker, no longer a combat pilot, but a computer hacker bent on destruction. For this is cyber war.

STEPHEN BADSEY
Waterloo is really just about the last major battle, before industrialisation and new technology starts to transform the nature of war. The way Wellington or Napoleon commanded at Waterloo had not changed significantly for thousands of years.

Julius Caesar, if he could have been brought to the battlefield of Waterloo could have commanded that battle. And you go from that to the trenches and the industrialised warefare of the First World War, just in a 100 year period. From thousands of years of battle remaining essentially the same, the impact of technology in just a hundred years transforms the nature of battle utterly.

NARRATOR
Industrialisation changed war, inflicting casualties on a scale that had never been dreamt of before. The first world war was mechanical, the soldier a working part of a greater machine, or merely a component on a conveyor belt of attack and death.

And the solution to industrial war? The development of more and more powerful technology of ever greater destruction.

ROBERT OPPENHEIMER
"Now I am become death, the destroyer of worlds"

NARRATOR
The atomic bomb remains the most potent expression of national military might and the ultimate symbol of industrial war.
The trouble is that we're no longer living in an industrial world - we have entered "the information age".

Clip of hackers copyright MGM

So is it really possible to wage war from a computer? Could a resentful teenager take on the might of national armies? In the movies the power of the hacker seems almost unimaginable, but as the scriptwriters discovered, film is often no more than a shadow of reality.

RAFAEL MOREU
I kept finding during the writing of it that there were things that er, I would just make up. I'd be like well, I guess feasibly if, and then I would like write it down and do it and then literally like, sometime later I'd hear about it being done...

Clip of hackers copyright MGM

There's an explanation of how this ship gets flipped, that the ballast system computers get infected with a virus, the ship thinks that certain tanks are empty when in fact they're full, and it fills and flips the whole tanker, and that's what the villain is doing. Well no one believes that one but it actually happened, that's where I got the idea - from the newspaper - I think it was in Portland or something, a tanker in the harbour just suddenly rolled and that's because there was a glitch in the computer system and it started flooding ballast tanks and suddenly swssh, it wasn't a tanker actually it was a cargo ship

Clip of hackers copyright MGM

DAN KUEHL
Western societies, the United States, western Europe, Scandinavia etc, have been in the past few decades become increasingly reliant, upon the smooth efficient functioning of electronic control systems for more and more segments of our daily life, our our livelihood, our political social economic processes; we have become dependent upon those electronic control systems; we have become quite accustomed to them functioning flawlessly all the time.

HOWARD FRANK
The group of people for whom the original Internet was developed, were a benevolent group of individuals who never really thought of things like overt attacks on the Internet, corruption of data by people thinking that that was a fun thing to do or a critical thing to do or a damaging thing to do.

Radio snap at The L0pht

NARRATOR
Fact or fiction? Heroes or villains? The world of the hacker is a real life movie set and possibly the new battlefield over which war could be waged. At a secret location in Boston resides "The Lopht" a seven member group - acknowledged in the US as a premier league hacker collective.

Continue radio snap at The L0pht

WELD POND
One of the things we find more interesting is searching around and seeing new digital modes people are using. So I'll search around and you can listen to it and you can kind of hear you know like when a fax machine starts up or a modem you hear all that beeping and buzzing. Well the same thing is happening over the radio. People are using the radio bands for all kinds of different things, pagers, mobile terminals like they use in police cars ambulances things like that, so we search around find what new services people are using, and we'll listen in we'll try to figure out if we can decode that digital data stream which is going over the radio and sometimes it's pretty interesting things.

NARRATOR
Systems which were once controlled by levers and switches are now controlled remotely by computers, networked over telephone lines or linked by radio waves.

This is the hard edge of the information age. If the computers go wrong, the technology which supports our lives will fail. And as the global network of computers called the Internet becomes the communication backbone of our society we become vulnerable to cyber attack - stop the networks and you stop the world.

STEPHEN BADSEY
Even with all our marvels, the most advanced society in the world is really only four meals away from anarchy, and if you could attack a society through its computers to cause the breakdown of the mechanisms the infrastructure which cause it to run, you *will* bring about mass deaths, and whether you do so indirectly or directly is still a consequence of your action.

| Title: | SCRIPT: "CYBERWAR" PAGE TWO |
|---|---|

MUDGE
This is our sixteen node massively parallel processing super computer. We picked this up out of the garbage of various large agencies, bit by bit they were throwing pieces out and bit by bit we picked it up until we had a working system. This was largely used for cracking military cryptography and encryption systems and schemes. As we go over here you'll see that just about everything from the L0pht has been picked up out of the dumpster. Since we don't have any money, we're not really funded by anything, we find things wherever we can. Companies will always try and stay at the latest technologies so that means stuff that's two years old, even if it's working get thrown out. So we pick it up and usually its completely working. So what if we're three years behind the technology curve, for us its absolutely fine. What we actually refer to this over here is technology reclamation.

MUDGE
We have probably about fifty different machines set up in here on networks. If we want to break into a system we'll set it up locally here and attack it. There are a couple of advantages to this. One, it keeps us out of jail, because we're not breaking into somebody else's systems that we don't own, and don't legitimately have access to.

And the other thing is, that it's in a controlled environment. So you know when you plug data in and you get data out, that was a direct result of your experiment. So it makes it much quicker and much easier to find the actual flaws.

HOWARD FRANK
You can be on the Internet without having anybody know that you're on the Internet; you can be behind another network for instance; you can have your own local network, and be connecting to the Internet, but nobody knows you're even there. So, we can't even predict its performance let alone know how to control it. Fascinating! Really an interesting concept. Nothing like it has ever existed as far as I know in the history of mankind before.

NARRATOR
The Internet began in the cold war climate of 1960s to protect communications in the event of nuclear attack. If parts of the network were destroyed information would still get through as packets of data could automatically re-route. And crucially there was no central control hub which could be targeted in a first strike.

But the physical safeguards of the cold war are the vulnerabilities of today. It's the very anonymity and anarchy of the Internet which throws its users open to software attack.

MUDGE
The seven of us could very trivially, take down the entire internet for the United States for Great Britain basically stopping communications between all the major network access providers. And this is a relatively well known problem. That would create a lot of difficulties. That would cause, overloads on to the other transit routes for communication, regular phone lines. It would cause problems for people trying to move large sums of money that are doing it over networks. It might cause, I don't... anybody who's hooked up to the network would experience problems.

INTERVIEWER
Easy to do hard to do?

MUDGE
Easy to do.

INTERVIEWER
How?

MUDGE
Take about thirty minutes... if that.

Pearl Harbour B/W film

NARRATOR
In 1941 the United States boasted one of the world's most powerful navies, but it was vulnerable to a new threat.
The devastation of American ships in the safety of Pearl Harbour by Japanese air bombardment is recalled in a new fear -
an "electronic" Pearl Harbour. The target would be the entire communication infrastructure of a state, bombarded by electronic viruses which would disable and destroy systems from the inside.

HOWARD FRANK
You can take down power systems and interrupt power supplies; you can take out emergency services; you could potentially get into the stock market computers and corrupt that data; you could potentially really do damage to the air traffic control systems.

You could think about any part of the way we run our society, and you can see that at the core of the way we run our society are electronic network's based on kinds of Internet like technologies, internet related technologies. And then you could think of what happens if those things fail.

NARRATOR
The allied success in the 1991 Gulf War, disguised a radical technological shift. Behind the Desert Storm paint, and the industrial rivets, lay critical information technology. The Gulf War appeared to be traditional, but history may remember it as a prototype for cyberwar.

MIKE MCCONNELL
There is no question that Desert Shield, Desert Storm was an intelligence war maybe I should it differently, an information war. We the United States and our allies could see the Iraqis when they could not see us. Their vision was blurred their hearing was impaired, and they had no capability to see what we could see. The result was overwhelming, and what I started to think about at that time was if someone applied those same techniques and capabilities against the private infrastructure of the United States, the banking system the power regulation system, the energy transportation system those kinds of things, because all of those systems are taking advantage of the information age. Therefore it introduces a level of potential vulnerability that we have not thought through as a nation.

NARRATOR
In 1992, a year after the Gulf War, two academics at the RAND Corporation, an American ex-government think tank, dared to think the unthinkable. That the industrial might of national armies might be as redundant as a Henry Ford production line.

In the corridors of power, their dramatic paper "Cyberwar is Coming!" was as unwelcome as it was unexpected.

JOHN ARQUILLA & DAVID RONFELDT
I actually received a phone call out of the blue from a fellow who told us his name but then insisted that we never use his name, and he said: "I've read this piece Cyberwar is Coming". And he said: "I think it's here". We said: "Well we think it's very nearly here also," and then he inquired as to how we could have written this piece without access to a lot of proprietary information and then he inquired whether it were possible to recall the academic journal issue in which it had been published and we said: "We don't think that's quite possible".

Yes, and he wanted to classify it. And thankfully we'd published before that all happened or could happen, and so we'd have been able to continue writing on the subject.

JOHN ARQUILLA
The whole technology is built around a notion of alienation from each other. People don't sit on their front porches and talk with their neighbours any more. The hacker is just a logical extension of this.

JOHN ARQUILLA
I think it's important for professional militaries to question the most central aspect of their being which is their forces. In the United States military, for example, we still have better than a million and a half troops in the various services. One has to ask whether even those numbers are still going to prove useful in the future. Do numbers make the difference on the battlefield or does knowing?

MIKE MCCONNELL
The argument has been made that information technology is a great leveller. I personally agree with that with that position.

JOHN ARQUILLA
Until about 1980 almost ninety percent of all research and development was done by the military or funded by the military. Today, early in the information age, the research and develop on defence related issues is already done ninety percent and a little more in the private sector. So this is a tremendous loss of control for the professional military.

MIKE MCCONNELL
The vulnerabilities for nations today, are profound, and it is very scary.
If you have an opportunity to understand the vulnerability and the potential threats from position I've had the good fortunate or, let's say the positions that I've occupied, you understand potential devastation that could be caused, by someone who specifically targeted, a nation's capability to function.

NARRATOR
Once an admiral, Mike McConnell is now a partner at Booz Allen & Hamilton, a global consultancy company which is adding cyber-advice to its range of services.

Woken up to security issues by financial losses, companies are turning to a fast growing network security industry, which is suddenly finding itself the guardians of its nation's assets.

MIKE MCCONNELL
Now you normally have the policy of the physical barriers fairly well thought out, fences and badges and a policeman to patrol in the physical parts of it, but what's different with the information age is you can reach through all of that and touch something valuable electronically.

DEAN RICH
It's an often occurrence that a large company will call and ask for immediate assistance, they've either had an internal security problem - somebody playing around with the system - or an individual coming from the Internet or a mysterious loss of money on a trading floor, and then people are called in to one find out what's going on, you now two - stop it. And then document the problems, get the fixes in place and if it's a hacker then start the process of collecting information to work with law enforcement.

MIKE MCCONNELL.
A terminal, either internal to a company or a terminal from a remote access, potentially allows one to network through tunnel or channel through an entire network to access data.

WELD POND
We're talking about things where peoples whole businesses are running on this software, and if a problem's found in something which can totally shut someone's business down, think... that's why we're serious.

page 2 of 3

Title: SCRIPT: "CYBERWAR" PAGE THREE

MUDGE
Think about buying a bullet proof vest. I mean would you like the company to go and say: "Here's a bullet proof vest we had a, you know we really just want to sell a bunch of them so it might not be tested tremendously well. If somebody finds a vulnerability in it later maybe we'll go back and fix it, but just you know wear it and feel comfortable right now" - no way! I mean that's what they're doing with the software out on the networks.

NARRATOR
In May 1998 the Lopht Collective went public, testifying to a US Senate Committee studying network security. Latter day Robin Hood's alerting the world to potential danger.

CNN REPORTER
These seven computer hackers make up Lopht Heavy Industries, a self described hacker think tank.

MUDGE
If you're looking for computer security then the Internet is not the place to be.

CNN REPORTER
Mudge and his friends laid out a Doomsday scenario, everything from complete disruption of electrical power, to transferring federal reserve funds. The session was heavy on possible dangers and very light on solutions.

The technology experts say that hearing from actual hackers instead of the usual academics, is a very good start.
Kelly Arena,CNN Financial News, Washington.

MUDGE
I think what scares us is that people aren't standing up right now, more people like us going "hey, you know you're all banking and you're all trusting this information tremendously and you're trusting it blindly." It's, trusting it isn't a bad thing, but be aware of what it is

NARRATOR
But in a world where fact and fiction mingle, who do you believe? Who do you trust? Security experts are the hackers of old, and many have perhaps not left old habits and friends behind. In cyberspace 'you need a thief to catch a thief', but do you know who the thief is?

DEAN RICH
There is a thrill, as you're doing it, even when you're authorised to break into a computer, sometimes your heart can speed up a little bit and you're kind of challenged with the thought of being caught. It's this kind of unique experience there. And then actually being caught, well then you can kind of get depressed that you weren't good enough but there is kind of a challenge there.

INTERVIEWER
Game over.

DEAN RICH
The game over, I mean you've been, you've been had.

Clip of hackers copyright MGM

NARRATOR
In cyberspace there's only a screen - a window onto game, movie, or reality. And who can tell which is which, or what's really possible in this confused, wild west world of the future?

MUDGE
Can you break into systems? Yes. Right now I mean are the systems running with swirlies and videos and music and you know you're controlling everybody's you know computer arms, left and right for broadcasting stations? Most likely not. But will that be in the future? Who knows? Are their groups of people at high schools who get together and hack? Yes. Definitely!

INTERVIEWER
Are there nasty people in security organisations.

MUDGE
Oh definitely.

MIKE MCCONNELL
My belief is that most of the damage today would be caused by an inside threat. Now, significant outside threat also exists, we normally think of it in terms of a hacker, but a hacker being someone who's just been able to penetrate any kind of the defences and get in and get access. Some hackers then could destroy data. It could be criminal intent, or it could be a terrorist, a terrorist group targeting some large infrastructure to be able to cause significant damage to a nation. So the vulnerability exists and then from its intent.

NARRATOR
Crime, terrorism, and war, all merge in this world where the power of nation states is declining while the power of individuals and dissident groups is increasing. For armies and businesses alike answers to security threats have to be found somewhere - and those answers might lie in the secrets of the oldest machines of all - living organisms themselves.

HOWARD FRANK
We've got two kidneys; we have multiple areas of redundancy cells regenerate themselves. We also have warning indicators; we have various kinds of amino acids and a variety of other kinds of protections that can alert us to penetrations, that can then start reacting. They can rebuild defences, they can move the biological organism out of the direct threat, adapt it and that can heal it after that. Now we're trying to do the same thing with these networks.

NARRATOR
Ultimately we could be entering an age where white knight viruses roam and destroy hostile, software assailants - our real world destiny, the outcome of battles in cyberspace.

But war is more than battle.

If developed countries can resist the threat of hacker attack, the concept of cyberwar might offer new hope - the potential end to armed battle as a part of conflict and the beginning of a new age of bloodless war where manipulating information and controlling people is more effective than destroying cities and killing soldiers. But nothing is ever really new, only reinvention of the old.

FRANCIS WOOD
We don't know much about Sun Tzu, or Sun Wu as he should really be called. He lived in the 6th century bc in China, and he left behind one work, the 'Sunzi Bingsa', the 'Art of War'. He does deal with how to move armies and how to fight sort of pitched battles and so on, but in the end it's it's cunning and the strategies of cunning that he's most famous for.

DAN KUEHL
We're learning lessons from Sun Tzu because he thought about how human beings function and operate and relate to each other. And as he said the acme of skill, is not to win a hundred battles through fighting, the acme of skill is to subdue your opponent without fighting at all.

FRANCIS WOOD
Classical Chinese is a very sort of pithy and punchy language if you like. It's very short and it's to the point, and it fits in very much... If people get, you know, if people talk "Confucius he said..." And there's some sort of pithy little maxim. Well Sun Tzu is exactly the same, and his pithy little maxims which are all about sort of defeating the enemy who is greater than you have been applied by people to all sorts of other areas of life in China and in the outside world. And it's been applied to business studies and sort of strategies for getting to the top.

DAN KUEHL
Is it possible to influence your adversary, influence your opponent, whether that is a nation state in a war, or whether that is a business in the financial world, or a political leadership or whatever, is it possible to influence them to your will, to your intent and your objectives without getting to the stage of bloody combat and fighting? That's what Sun Tzu offers as a paradigm to examine in the future, and that's one of the reasons why we study him.

STEPHEN BADSEY
If increases in terrorism, if increases in computer hacking, information warfare create that kind of society which a number of military theorists are afraid it will create, that breaking down of the boundaries between what constitutes a soldier and what constitutes a civilian will produce a state which we will not perhaps call warfare, but it certainly will not be peace.

NARRATOR
But in the end how do you define war at all? Certainly not everyone is so sure the information age will lead to a future of bloodless strategy and diplomacy.

NEIL MUNRO
If a cyberwar is fought, without politics or ideology we call it vandalism or theft. It's politics that make it a war, and if the political struggle is vicious and nasty and deep enough to justify hacker wars, deep enough to justify good old soldiers fighting for political gain, otherwise it's just called commerce and litigation.

STEPHEN BADSEY
Because warfare is so violent, because it kills people, there's always been a search throughout history for what might be called the philosophers stone of warfare, which would not cause many casualties - the belief that surgical air strikes might produce the short sharp successful war resulted in the mass bombing of the Second World War.

NARRATOR
No one knows how cyberwar will change conflict, but we're going to have to be cleverer than ever to resist its threat when it comes. For history has told us that new technology has never eased war, let alone replaced it - it's only added, unpredictably, to a fighter's existing arsenal of attack.

STEPHEN BADSEY
Even in the Gulf War of 1991, although surgical, the overall weight of bombing was conventional explosive bombs of great destruction. And there is no specific reason to think that information warfare will provide the technological solution to what is essentially the political and social problem, of the fact that people feel the need to go to war and are extremely inventive about it.

PRODUCTION TEAM