CHAPTER 24

# THE JOKER IN THE PACK

## CYBER-ATTACKS

Everything in the nuclear world is made possible by computers, ranging from tiny microprocessors to immensely powerful supercomputers. All aspects of warfare in advanced countries rely upon software, but software can be interfered with.

As computing becomes more complex the clever art of interfering with software will become increasingly dangerous. A major aspect of warfare will be the ability to play havoc with the other side's computers. Major nations, including China, have numerous ways to break into computers, read data, change data, and hide different types of viruses. Malicious attempts to interfere with software are referred to as cyber-attacks. When done on a large scale, they constitute cyber-terrorism or cyber-warfare. Cyber-attacks may be planned by top intelligence or military organizations, but often isolated hackers with strange motives and diabolical skills do their own interference with systems.

## HACKERS AND SUPER-HACKERS

Around 1980, when personal computers were a new type of toy, many young people entertained themselves by interfering with other people's computers. The internet spread rapidly and some of its users mischievously explored ways to misuse it. However the mischief turned into the capability for serious damage. The internet became widely used academia and business, and acquired hundreds of millions of individual users. The world-wide web was designed so that many people around the world could use it. There was great excitement about what it could grow into and how to make it spread worldwide, but there was almost no attention to security in its basic architecture. Revolutions don't want anything to slow them down.

Hackers attacked computers, for example in banks or government, so computer departments everywhere installed protective measures. Protection from hacking is a standard aspect of installing computer systems. Most attempts at malignant hacking were blocked and most casual hackers abandoned their pastime, but some of the most brilliant hackers dedicated themselves to penetrating the protection.

There are many low-level hackers with a variety of motives, but also a different breed of hacker evolved, which I will refer to as super-hackers. These top hackers are a strange breed, often loners, living in endless layers of clutter, getting a thrill from breaking into the most secure systems and leaving "Trojan horses" there, which they might activate at a later time. Some super-hackers are more brilliant than chess champions and sometimes seek out other super-hackers on global networks. Global communities of hackers evolved, with the superstars often knowing of each other's reputations. Many super-hackers want to prove their brilliance to other super-hackers.

There is much literature about hackers and their psychology, but super-hackers are a world apart. They are not necessarily malicious; their activity is more like a sport or a deep cerebral game. In the hidden world of super-hackers there are many strange people. There doesn't appear to be a criminological theory or true understanding of why they hack. The motivation of top hackers may always be a mystery.[170]

Defense against top-level cybernetic attack will be as intellectually challenging as the attack itself. In the super-hacker community there are there are stars of attack and defense, sometimes there are battles between them. A surprise attack can be often devastating and totally without warning – an intellectual Pearl Harbor.

## MALWARE

Software can be designed so that it travels through networks and causes trouble; existing software can be interfered with so that it malfunctions. Such software is referred to as "malware."

Software that is secretly hidden so that it can be activated at a later time is referred to as a "Trojan horse." A "trapdoor" is software maliciously added to a program in order to make it easy for a hacker to penetrate it in the future. Most 14-year-olds know the names of malware, such as "logic bomb", "virus", "worm", "packet sniffer" and "keystroke logger". A logic bomb could shut down a network or erase all the data in a computer. A virus could travel through a network and infect many computers with malware, or leave Trojan horses. A worm is designed to infect a computer in such a way that it sends the worm to other computers, so that the number infected grows from thousands to millions around the world. A packet sniffer could illegally inspect packets of data looking for information. A keystroke logger could secretly record what is entered into a computer on a keyboard. A common type of malware can flood a server with a severe overload of requests so that the server cannot provide its intended service.

There are many variations on these mis-uses of software.

Trojan horses can be hidden in existing code in a variety of ways. As software is being developed it is usually modified many times. As this happens, some code becomes unused; it becomes dead code. A hacker observing a system in use can identify the dead code and replace it with malware. This intruding code is often not detected. An innocent-seeming system can exist indefinitely with hidden Trojan horses.

In normal text each letter is encoded with eight bits. There are 256

possible combinations of 8 bits, and most of them are not used. A hacker could replace the unused ones with code that would appear blank if printed. The spaces between words or paragraphs could contain a rich collection of illicit code. This page of this book might have 400 blank spaces, providing 1024 bits for potential malware. The world could be flooded with malware that nobody would notice.

In 2010, the Wall Street Journal stated that the American electrical grid had been the target of thousands of known hacker attacks.[171] Many logic bombs had been left in the software that is essential for the operation of the grid: there was evidence of widespread hacker investigation of the grid, as though some organization were mapping the territory.[172] There can be no evidence of where such malware has come from. Hackers might route their attacks through a country such as Bhutan, then St. Lucia, then Bolivia, so that it can be traced back to those countries but not to its country of origin. The hackers can be invisible and anonymous. Recently North Korea has been finding high-IQ kids and training them to be highly skilled hackers who can carry out cyber-attacks against strategic international targets. The CIA and National Security Agency have probably trained many super-hackers.

## PIPELINE EXPLOSIONS

In June 1981 at a summit in meeting in Ottawa, French President Mitterrand shared a highly explicit set of intelligence files with U.S. President Reagan, showing that the soviet KGB had been infiltrating American research centers and corporations and stealing technology information of great value to the USSR.

At that time the USSR was building its trans-Siberian gas pipeline. This pipeline is 2,800 miles long and has a diameter of almost 5 feet. The pipeline can carry 32 billion cubic meters of natural gas per year and it is intended to produce $8 billion per year in gas revenue. It has many compressor stations with more than 60 miles between them. Exceedingly complex software is needed to control the pump pressures and valves so as to obtain the maximum flow. The USSR did not possess such software. It tried to buy it from the USA but the Reagan administration prevented U.S. companies from selling supplies to the

soviets for the pipeline, so the KGB planned to steal it from Canada.

The CIA became aware of this, so it set out to hide a "Trojan horse" in the software. The pipeline equipment and its software passed soviet inspection and the Trojan horse was not detected. Engineers steadily brought the pipeline into operation. When a section of the pipeline was operational at full load, the Trojan horse was activated that could reset pump speeds and valve settings. In one sixty-mile section of pipeline it increased the entry pressure and blocked the exit. It made the pressures between compressor stations far beyond those that the pipeline construction could handle, and a massive explosion occurred. The NORAD (North American aerospace defense command) monitoring stations detected it and caused fears that it might be a nuclear explosion, but satellites confirmed that this was not the case. It had the power of a small nuclear weapon – about three kilotons of TNT – and was the largest non-nuclear explosion ever seen from space

After it occurred, all the other pipeline software that the USSR had stolen became suspect. The work of thousands of Russian technicians and scientists was stopped or delayed. There were several other smaller pipeline explosions. On June 4, 1989 at 1:15 pm a massive pipeline explosion occurred in the southern Ural mountains. There was a fireball large enough to be seen sixty miles away. The explosion blew out windows in Ashai, eight miles away. The pipeline went along the track of the famous trans-Siberian railway. Unfortunately two trains were passing each other as the explosion occurred, with 1,200 passengers aboard. Hundreds died and more than 700 were rushed to hospital, many with terrible burns. It was the worst train disaster in soviet history.[173]

## HACKING INTO DEFENSE SYSTEMS

There have been multiple attempts to hack into defense systems. Some defense servers have been rendered inoperable, so that there is denial of service. The massively expensive fighter of the future, the Lockheed Martin F-35 Joint Strike Fighter, depends on extremely complex software of more than a million lines of code. It is believed that some of this was stolen by a hacker.[174] This raises the possibility that the hacker could leave a Trojan horse in the software that might be

activated when the plane is in battle.

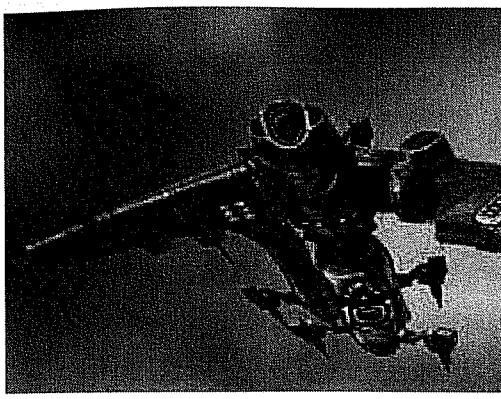
There are many potential targets for cyber-attacks. As commented earlier, in 2007, Israeli fighters destroyed a Syrian reactor protected by an extremely expensive air defense system, provided by Russia. Before the raid, the defense system was hacked into by the Israelis so that it did not observe the attacking aircraft. In 2010 a hacker attack with a clever virus put many of the Iranian uranium enrichment centrifuges out of action.

Defense departments are planning for a full-scale cyber-attack. This would have very different characteristics from a traditional attack. First, it would happen almost instantaneously. The signals initiating it would travel to their targets in a fraction of a second. Second, if it were an all-out attack, it could devastate a modern nation that was ill-protected (as most are). Third, the attack may not be visible; it may be prepared for by leaving thousands of undetected Trojan horses. Fourth, it may be uncertain who caused the attack. The attacker wouldn't leave a calling card. It may not be a non-state organization or a crazy person, or someone seriously upset by the current state of affairs. A cyber-crisis might come from a person or group planning to make the stock market plunge and buy at the bottom. The capability for instant attack is part of our future.

## ANYTHING GOES

We described the present era as one where "Anything Goes." Crazy hackers, cyber-attacks, a proliferation of robot delivery systems, dirty bombs, the ability to build amateur nuclear bombs and use cheap drones, with many such technologies dropping in cost -- these are all part of the nuclear Era 3. If nuclear weapons, and the fissile materials with which they can be built, are not eliminated, there will be growing dangers of nuclear catastrophe.

Cyber-attacks will always be possible where the origin can't be traced – super-hackers or cyber-mercenaries, devilish college drop-outs, intellectual criminals, burnt out Wall Street stars, genius loners living with their cat, or the twenty-first century version of the Unabomber.



*The problem with "artificial intelligence" is that it isn't intelligent. It has no flicker of common sense.*

The techniques of attacking will become increasingly automated and clever. It will be essential for countries around the world to join forces so that they can share intelligence and mutually protect one another from potential cyber-attacks, but there will probably always be rogue countries. It will be necessary to have malware nonproliferation treaties and mutual inspection, just as we have nuclear nonproliferation treaties with mutual inspection. There will be complex tools for detecting trapdoors and Trojan horses. However, in my observation of discussions of this in high circles, it seems to me that the participants do not come close to understanding the mind of the super-hacker or the extraordinary intellectual depth of possible attacks.

The danger of illicit hacking will made much worse by the spread of artificial intelligence. Artificial intelligence will be used (among many other things) to make robotic weapons more autonomous; in other words they can take actions without a human at the controls. There will soon be swarms of small weapons using artificial intelligence.

The proliferation of drones, robotic delivery systems, and any "autonomous" weapons, makes it extremely dangerous to have small nuclear warheads. Many means of delivery can be obtained from commercial catalogues. Nuclear systems that were ultra-secure in the past may suddenly become difficult to make secure, partly because of the unpredictable capabilities of super-hackers. "Artificial intelligence" greatly increases the power of super-hackers.

In the first era of the nuclear world, missiles and command-and-control systems were designed with knowledge of who the enemy was. Now a major power may not have that luxury. The technology was extremely expensive but highly secure (although they was a plague of false alarms). In the Second Era there was no comfort that the new nuclear nations such is Pakistan and North Korea had systems as well thought out and secure as those of the USA and USSR. In the third era there is no clarity about who the enemy is – it might be an amorphous underground organization not associated with one country, possibly large and multinational – global, perhaps – with carefully hidden cells of activity. A Mafia of the future may have nuclear devices and

mercenary super-hackers.

A cyber-skilled enemy may be large or small; it could be one individual or an organization of isolated cells. It might be within one nation, or globally scattered. It might be religious or, perhaps, a suicide bomber. It might be diabolically intellectual or devoid of intellect. It may be angry and emotional, or it may be calculating with a profound set of objectives. It may have a shoe-string budget or be massively financed.

When Apple released the iPhone it had an exclusive partnership with AT&T, and this exclusivity was built into the iPhone, locked with what was thought to be unbreakable security. A 17-year-old from New Jersey, George Hotz, with great ingenuity, hacked the iPhone. He made a videotape in his parents kitchen and announced "This is the world's first unlocked iPhone". The video had nearly 2 million viewers on YouTube.[175] Sometime later he attacked Sony's PlayStation 3, which had never been hacked. The PlayStation 3 was left wide open. Hotz hacked the most "unhackable" devices of his time. The Sony Corporation of America created a new position – a senior vice-president for security and privacy, but eventually he admitted "in the end it must be recognized that no system is absolutely foolproof.[176]

Super-hackers want medals, like military people, and a top medal might be a demonstrable ability to break into a nuclear war system. A super-hacker might dedicate months of effort to finding out how to put a nuclear defense system on alert and show the results to super-hacker colleagues. He or she might find a way to make Pakistan go to a high level of nuclear alert, and then watch what happens in India. When one country's system goes on alert, those of other countries may go on corresponding alert. A top qualification might be to make a nuclear system go from DEFCON 5 to DEFCON 4; perhaps even DEFCON 3. (Curiously a major international annual convention on hacking is called DEFCON.)

In the world of cyberspace, artificial intelligence and super-hackers, nothing is certain. It becomes insanely dangerous to have Era 3 nuclear weapons.