[21]

Cyberwar

> Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts… A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.
>
> **WILLIAM GIBSON,** *Neuromancer,* 1984[1]

The other form of information warfare was to interfere with the information flows necessary to keep modern military and civilian systems working. In this respect it was as much an aspect of 'cyber war' as 'hybrid war'. The idea of cyberwar was a natural inference from the digital revolution. If all military activity depended on the rapid collection, processing, and transmission of data then should not that be as important a focus of attention as launching strikes or blunting enemy attacks? What if one side suddenly found itself in the dark, with screens either blank or full of misleading information, and was unable to send out orders to local commanders or else had these orders substituted by false instructions? In such circumstances even the strongest military machine would be left helpless and hapless. Take the analysis a step further and look beyond military activity and then an even more alarming thought developed. If all key functions of a modern society—energy, transport, banking, health, and education services—depended on these flows of information, might it be possible to bring a country to its knees without firing a shot? Stopping the flow would be like pulling out a gigantic plug. Everything would go dark, screech to a halt, or clatter and bang, leaving an economy in tatters and a society struggling to meet its most basic needs.

Unlike other visions of future war this was only in part a question of imagining how technologies might develop. The vulnerabilities created by the digital age were evident in everyday stories of viruses and worms infecting computers, of foreign agents, disgruntled employees, would-be extortionists, or just curious youngsters hacking into supposedly secure systems, undertaking acts of malicious interference, sometimes no more than an irritating nuisance, sometimes causing serious damage and disruption. There were reports from past conflicts of enemy air defences caught napping, command systems confused, and propaganda opportunities exploited. From the start the question was not one of whether or not there was an issue here but how the risks and opportunities were to be measured, and how the relationship between this new arena of conflict and the nature of warfare as a whole was to be conceptualised. The problem appeared as being somewhere on a spectrum from the equivalent of a nuclear war to a minor inconvenience.[2]

There was a link to the post-Second World War thoughts about a coming ‘push button war’, in which guided missiles would rule and armies might become redundant.[3] As we saw in Chapter 7, once nuclear warheads were added to these missiles and they acquired intercontinental ranges, two types of fears began to dominate the debate on future war. The first was whether one side might be able to configure its nuclear forces so as to launch a disarming first strike, transforming an apparent balance of power into one-sided dominance. The other, even if there was no premium in striking first, was the potential interaction of human failings and technical malfunctions that would turn an otherwise manageable situation into a global cataclysm. Norbert Wiener, who had developed his ideas on cybernetics from his work on anti-aircraft weapons during the Second World War, had become increasingly alarmed at the implications of developing air defence systems which had to work so quickly that there was barely a chance for human intervention.[4] The theme of lost control over a situation hurtling towards tragedy was the basis of the movies *Dr.*

Strangelove and *Fail-Safe*.

IN 1979 TWO SCREENWRITERS, LARRY LASKER AND WALTER Parkes, developed an idea for a movie based on the interaction between a dying old scientist and a smart, rebellious teenager, which soon revolved around their shared understanding of computing. Aware of stories about how the North American Aerospace Defense Command (NORAD) could mistake innocent signals for an incoming Soviet attack, they toured NORAD. There they met with the commander who, on their telling, shared his concerns about the risk of over-automated decision-making. They also learnt about simulated war games. Out of this came the core plot of the movie *WarGames*, released in 1983. A teenager, David Lightman (played by Matthew Broderick), hacked into a supercomputer designed to predict outcomes of nuclear war known as War Operation Plan Response (WOPR). Lightman noted a number of familiar games but then saw one called 'Global Thermonuclear War' which he decided to play. This turned out to be a programme that could convince the systems operating nuclear missiles that this was the real thing. When he realised what he had done, and after arrest by the FBI for the hack, Lightman reached the embittered, dying scientist who had invented the programme to persuade him to give him the clue to turning it off. This was done seconds away from catastrophe. As WOPR was a learning machine it could realise that some games led to futility, which became a metaphor for mutual assured destruction. After this point was reached through a drawn game of tic-tac-toe the computer had the last line: 'A strange game. The only winning move is not to play. How about a nice game of chess?'[5]

As with the doomsday machine in the earlier movies, the plot depended on a prior decision to give deterrence a form of automaticity that prevented human beings interrupting the launch sequence. The movie opened with a surprise drill in which, when confronted with an incoming nuclear attack, the USAF personnel supposed to turn the keys to launch retaliatory strikes failed to do so. Instead of a Germanic think tanker the villain now was an all-American systems engineer who, against the advice of the NORAD commander, insisted that the launch process must be automated, which is why WOPR had this crucial role. When the movie was released the Pentagon was at pains to point out that it was misleading about NORAD’s role and also the possibility of the nuclear arsenal being out of human control. Whether or not the intent was to make a film in the spirit of *Fail-Safe* or *Dr. Strangelove*, alerting the audience to the risks of an inadvertent nuclear catastrophe, the main thought left by *WarGames* was the ease with which an outsider might hack his way into the most vital computer networks, highlighting the risks posed by remote access and simple passwords. This was the message taken away by President Reagan, a friend of Lasker’s parents, who was invited to an early showing and was sufficiently disturbed to ask officials whether this movie had a basis in any conceivable reality. As the issue was investigated it turned out to be more serious than had been realised, leading to a set of studies into what was then described as ‘Telecommunications and Automated Information Systems Security’.[6]

This was a time of exploration into this developing networked world of information, a disembodied place where real things could be made to happen by anyone who could gain access. *WarGames* had pointed to the possibility of a war starting from within cyberspace. Yet not only was the term itself still unfamiliar, but the prefix also already had connotations of cyborgs, man-machine combinations with extended powers.[7] The prospect of computers gaining the upper hand in some future conflict was linked naturally to the idea of robotic warriors, a standard feature of science fiction.

Robots were introduced in a 1921 play by Czech writer Karel Čapek about a company that sold machines that looked like people as forms of slaves. He got the term from ‘robotniks’ or surfs. As he was aware that these robotniks had rebelled against their masters in 1848, Čapek had his robots also turning on their human masters, introducing a regular theme into science fiction.[8] As mechanical devices increasingly performed simple but demanding household tasks during the twentieth century it was natural to consider how they might take over as soldiers. In 1968 a professor of Mechanical Engineering described how it would not be long before radars would be able to propel themselves forward, seek out enemies and kill them. ‘A line of such robots spaced twenty metres apart might be deployed to move at fifteen kilometres per hour through a jungle and destroy all men encountered there'. Within 'a few years' men would 'cease to be valued in battle'. They would complicate matters because they would lack comparable 'information storage, decision-making, sensory input and pattern-recognition'. The human role was likely to be to 'stand helplessly by as a struggle rages between robot armies and navies, and air and rocket forces'.[9]

In the first article to talk of 'cyberwars', published in 1987, robots dominated the scene. They were fearless and irresistible, pushing away any poor humans sent to confront them. If everything was automated then future wars would be between machines with artificial brains, with their controllers hidden away in command bunkers.[10] Cyberwar dominated by robots that 'do much of the killing and destroying without direct instructions from human operators' was also the theme of an article in the *Bulletin of Atomic Scientists* in 1992. The idea of a network was still missing. What was alarming about these systems, whether crewless tanks or anti-missile satellites, was their autonomy.[11]

The team of Lasker and Parkes released another movie in 1992 called *Sneakers*. It had been conceived while *WarGames* was being made, and took on a similar theme, this time involving a device stolen from the National Security Agency (NSA) that could decode all encrypted data. It did not make the same impact, except for the fact that it was watched by the NSA's head, Admiral Mike McConnell, who was taken by a line in the script:

> The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeroes, little bits of data. It's all just electrons… there's a war out there, old friend, a world war. And it's not about who's got the most bullets. It's about who controls the information: what we see and hear, how we work, what we think. It's all about the information.[12]

This vulnerability had already been identified in a 1991 report by the National Research Council:

> We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital

> information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps more alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.[13]

An IT entrepreneur from Tennessee, Winn Schwartau, first in a journal article, then in Congressional testimony, and eventually in a self-published novel, *Terminal Compromise*, highlighted the danger. He told Congress: 'Government and commercial computer systems are so poorly protected today that they can essentially be considered defenceless'. Drawing on the unavoidable analogy, he spoke of 'an electronic Pearl Harbor waiting to occur'.[14] The plot of his novel had at its centre a Japanese survivor of Hiroshima, seeking revenge against the United States, and involved 'Arab zealots, German intelligence agents and a host of technical mercenaries' identifying 'the weaknesses in our techno-economic infrastructure' to land blows that hurt the US economy, taking in Wall Street as well as the carmakers Ford and Chrysler.[15] In their 1993 book *War and Anti-War*, the Tofflers quoted Schwartau warning of an electronic Pearl Harbor and others alarmed about the possibility of 'info-terrorists'.[16]

The idea of the electronic Pearl Harbor gained more traction in policy circles following a 1995 crisis simulation led by RAND analysts Roger Molander and Peter Wilson who had been engaged in a series of exercises on nuclear warfare. They put to decision-makers a developing crisis and asked them to consider issues of escalation. Now they envisaged a series of attacks that disabled a Saudi Arabian refinery, derailed a high-speed train, crashed an airliner, took down power grids, and put CNN offline. An 'electronic Pearl Harbor' meant 'that some country or terrorist might attack US computers in one sudden, bolt-out-of-the-blue strike, causing death, destruction, and mayhem.'[17] Policymakers appeared to be at a loss to know how to respond, yet could not deny the problem. 'The electron', explained CIA Director John Deutch, 'is the ultimate precision guided weapon'.[18] In his confirmation hearings as Secretary of Defense in 2011, Leon Panetta deployed the analogy yet again to warn of a 'digital Pearl Harbor'. A former chairman of the Joint Chiefs of Staff warned the same year: ‘The single biggest existential threat that’s out there, I think, is cyber.’[19]

The persistent use of the most searing experience in recent American military history to frame future attacks pointed very deliberately to the potential for surprise. But Pearl Harbor, of course, was not a knockout blow. The US recovered and defeated the perpetrator. This hypothetical case, therefore, raised exactly the same questions of why an enemy would do this, how they would follow up any achievements in the initial strike, and what political purpose might be served. There was also the question of how confident the attacker could be that all would work as planned. A lot would need to be known not only about the target’s vulnerabilities, and whether defences had been improved, but also the degree to which the target was dependent upon the systems being attacked. As Wilson, one of the designers of the RAND simulation, observed, these were more weapons of mass disruption than mass destruction, and that ‘by painting doomsday scenarios, government officials lose credibility and, over time, their ability to influence the public.’[20] The issue was also perplexing because while some attacks might cause loss of life most would not.

As one group worried about how the United States might take advantage of the vulnerabilities of information systems to mess with enemies, others worried about how the same vulnerabilities in their systems might allow the enemy to mess with them. Given the resources allocated to this issue it could be assumed that the Americans were well able to interfere with the systems of others. Small but significant acts illustrated the possibilities. First Iraqi and then Serb air defences were degraded by messing with their software. The Israelis did something similar with Syrian air defences when they took out a nuclear reactor under construction in 2007. The Stuxnet virus, probably a joint US-Israeli project, was designed to set back uranium enrichment in Iran by disabling centrifuges.[21] This had some effect but also showed how hard it was to stop these attacks spreading away from the original target. The virus was noticed when non-Iranian systems were hit.

Every time national systems were tested to see how well they could defend against interference from others, they were found to be wanting, and for all types of networks, malevolent hacking became regular. In 2014 there were almost 80,000 security breaches in the US, more than 2,000 of which resulted in lost data. Hackers stayed inside the networks they had breached for an average of 205 days.[22] Behind the attacks were criminal groups and political activists as much as governments, although the line between them could get blurred. They normally appeared as 'bolts from the blue', but they tended to be damaging more than crippling, and usually had far more to do with the theft of business secrets, or malicious attacks on individuals or companies, than with international affairs. Sometimes it was difficult to work out what was deliberate interference and what was a consequence of the fragility of some of the connections. Internet services regularly went down because of accident or error. In one incident a 75-year-old Georgian grandmother cut off the Internet to Armenia with a shovel, almost leading to an international incident as Russia was at first blamed.[23]

The assumption that it would be impossible to attribute attacks was challenged as the forensics improved.[24] The US became more ready to assign blame, whether it was a North Korean attack on Sony Corporation for a movie which considered the possibility of the assassination of its leader, or, more seriously, Russian attempts to swing the 2016 presidential election. In these cases the US government also spoke openly of retaliation. The US became explicit about the deterrence aspects of its cyber-strategy in the military sphere as well, threatening to 'use cyber operations to disrupt an adversary's command-and-control networks, military-related critical infrastructure, and weapons capabilities.'[25]

As with all new developments the question was whether this was a way to get a decisive result in a conflict or just another means of engaging in a dispute without necessarily being able to bring it to a conclusion. In earlier debates about the impact of first air power and then nuclear weapons a distinction had been drawn between strategic and tactical effects, with the former making possible a decisive victory and the latter only having their effects as a result of working with other types of forces and in particular armies. Arquilla and Ronfeldt sought to redefine cyberwar in a 1993 article away from automated forms of physical forces to the centres of knowledge and communication at the heart of modern military and social systems.[26] This fitted in with a wider trend in thinking about warfare, represented as a shift from mindless attrition, which relied on physical destruction, to more intelligent manoeuvrist strategies, which depended on getting inside the enemy's head to confuse and demoralise.[27] The next shift was from interference with the information processes that kept military systems working to those that did the same for a whole country.

According to Arquilla the purpose of this article had been to stress tactical effects, showing how disruption of networks might interfere with one side's ability to fight a conventional war, while they were sceptical about the 'strategic attack paradigm' which saw the attacks being directed against national information infrastructures. Yet, he observed, the academic and policy debate soon got drawn to 'a kind of information analog to strategic bombing'.[28] This was not to deny the evident tactical value in exploring the weaknesses in enemy forces. One general reporting on his experience in Afghanistan described how he 'was able to use my cyber operations against my adversary with great impact.… I was able to get inside his nets, infect his command-and-control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations.'[29] The challenge lay in showing how cyberwar should be viewed strategically. The issue was not one of how hurt might be caused but of linking the hurt to a political purpose, especially if that was the sole form of attack.

To do major harm would require substantial preparation, including considerable research into the system being targeted to identify its vulnerabilities, in the hope that this would not be detected, and then customising a package to implement the required sabotage. Whatever the options developed during prior reconnaissance there were likely to be major uncertainties about their effectiveness until an attack was actually launched, including whether the target had noticed that its systems had been penetrated. These attempts therefore could not be spur of the moment decisions but must be prepared well in advance of any attack, and the options might degrade quite quickly. The adversary might have been doing its own probing and found evidence of a planned offensive. A state picking up on an adversary's preparation might decide to make a fuss or simply make any attack harder to execute and wait to see what happened. None of this might be visible other than to those directly involved.[30] These uncertainties would all make cyberweapons an uncertain foundation for aggression.

An imagined cyberwar was the natural culmination of a yearning for non-kinetic wars, forms of engagement that would disarm and disable a whole society without mass slaughter. This is why there was continuing anxiety about the worst case of ‘an electronic Pearl Harbor’, with a sudden attack leading to social and economic breakdown. The everyday reality, however, was more of a level of threat that was routine and ubiquitous. Not only was it the case that any conflict, even one that was largely non-violent, exhibited cyber elements, but also that this had become almost a preferred form of engagement, precisely because it was relatively minor. It provided opportunities for soft forms of coercion, signalling concern, or hinting at some future escalation. This is one way to interpret Russia’s electronic bombardment of Estonia in 2007 and Georgia the next year.[31] In neither case was the effect of the denial of service attacks lasting, but both served as warnings of what might be done in the future. In this way states behaved ‘more and more like individual hackers, carrying out crimes of petty vandalism, theft, disruption, destruction, and even cyber-bullying.’ It was an unrestricted form of conflict without obvious limits, probing while avoiding excessive provocation, but still undertaken at a level inconsistent with responsible state behaviour.[32] In this respect, cyber-attacks became more analogous to irregular war than strategic bombing, another way to harass and subvert, to confuse and annoy, but not a way to win a war.