3
Strategic Information Warfare: An Introduction

Gian Piero Siroli

> . . . Attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy's army without fighting is the true pinnacle of excellence
>
> (Sun Tzu, 'The Art of War', about 500BC)

3.1 Introduction

Since the mid-1980s a very rapid evolution of information and communication technologies (ICT) has taken place, together with a worldwide proliferation of information systems. The rapid expansion and integration of telecommunications technologies, computer systems and information processes has deepened and broadened the Information Infrastructure (II) at every level of society and, in particular, in western industrialized countries; citizens, economic activities and state organizations are increasingly reliant on information technologies (IT).

This evolution process has many positive aspects. However, it should also be analysed from the point of view of an increasing dependence on the new networked global II currently under construction and, as a consequence, also in terms of vulnerability and possible security implications. Widespread reliance on information-based technologies may be driving society towards an unprecedented degree of global connectivity and interdependence. New vulnerabilities, which can be exploited at various different levels, are induced by the convergence and increased overlapping of the traditional critical infrastructures of a country (for instance, vital infrastructures like the energy distribution systems or the emergency services) with present-day II being prone to electronic attacks.

The IIs, consisting of information systems and telecommunication networks with all their related technologies, is also becoming increasingly important for the defence policies of many countries since it might become a significant military target under certain conditions. Moreover, it should not be forgotten that information and disinformation has always been a key factor in war. The exploitation of advanced IT in the military field is driving the development of new warfare techniques, raising the problem of both national and international security.

This chapter is an introduction to the subject of strategic IW – in other words ITs seen in the context of national and international security; it describes possible vulnerabilities of critical infrastructures in modern developed countries. The report released in 1997 by the US President's Commission on Critical Infrastructure Protection (PCCIP) will be taken here as a case study and some of its main conclusions will be analysed and discussed.

What does IW mean? From a general point of view, it includes the actions taken to achieve superiority by affecting an adversary's information, information-based processes, information systems and computer-based networks, while defending one's own domestic II. In other words it is the set of activities intended to deny, corrupt or destroy an adversary's information resources; it includes both offensive and defensive operations, often with a significant overlap between the two.

3.2 Context

The United States of America (USA) is probably the most advanced country in the world in terms of IT. At the same time, it is also the one that is most dependent on communication infrastructures, with the consequence that it is far more vulnerable than other countries with respect to IT. Particularly in the USA, various activities and research programmes concerning IW are taking place at many levels, addressing the questions of protection, assurance and the survivability of vital infrastructure.

These activities include a series of official steps taken by the US government; we will mention here only some of the most important ones to exhibit this trend. In January 1995 the US Secretary of Defense established the Information Warfare Executive Board 'to develop and achieve national IW goals'. Six months later, the Presidential Decision Directive 39 (PDD39) set the policy concerning terrorist threats, which also includes activities relating to IW. In July 1996, the Executive Order 13010 established the President's Commission on Critical Infrastructure Protection (PCCIP), setting the goal of assessing 'physical and cyber threats to national vital infrastructure' and developing 'strategies to protect it'. At the same time the Infrastructure Protection Task Force (IPTF) was created, 'to increase coordination on infrastructure protection'.

The key elements of US policy concerning critical infrastructure protections were defined in the PDD 63, released in May 1998. This directive was followed by the creation of two agencies – the National Infrastructure Protection Centre (NIPC), located at the FBI, and the Critical Infrastructure Assurance Office (CIAO) at the Department of Commerce. At the same time other projects were proposed, for example, the Federal Intrusion Detection Network (FIDNet) to protect government and key private sector nodes through widespread system and network monitoring.

In July 1999 the Executive Order 13130 established the National Infrastructure Assurance Council (NIAC). Later on, in January 2000, the US administration issued a 'National Plan for Information Systems Protection', describing the new dependencies and threats. This proposed a public – private partnership and training programmes to achieve cyber defence; this plan officially included FIDNet for the protection of federal civilian agencies whose funding requests sum up to $10 million in the Fiscal Year 2001. The FIDNet initiative, a warning system to monitor critical computer networks, was later abandoned and replaced. However, the goal is to sustain the ability to alert NIPC in case the Federal Computer Incident Response Capability (FedCIRC, a central coordination and analysis facility dealing with computer security related issues) suspects any hostile activity. In 2002 the US 'President's Critical Infrastructure Protection Board' published a report on 'The National Strategy to Secure Cyberspace' and the Joint Economic Committee of the Congress released 'Security in the Information Age', describing a range of perspectives on infrastructure protection. Since then, many more activities have been developed in this context at many levels.

Similar programmes began later in Europe, albeit with a different aim. In 1997 and 1998 four workshops were held in consultation with industry, academia and public authorities to prepare for the establishment of the European Dependability Initiative within the Information Society Technologies (IST) Programme, to be managed by the Information Society Directorate-General (DG) of the European Commission. The goal was to raise and trust and confidence in systems and services, addressing dependence on ICT and new vulnerabilities.

In 1999 the Scientific and Technological Options Assessment (STOA) team commissioned four studies, in response to a request from the Committee on Citizen's Freedom and Rights, Justice and Home Affairs. The first study concerns state-of-the-art electronic surveillance via Communication Intelligence (COMINT) for global interception capabilities. The second study deals with encryption and cryptosystems, the mechanisms used to protect against interception of communications. The third study examines the legality of intercepting electronic communications, reviewing the existing policies and international agreements. The final study analyses the economic risks arising from the interception of communications. These activities are focused in a slightly different direction than the US initiatives and include data protection and the confidentiality of communications; it is an indication that these technologies have important implications in very different sectors. It is appropriate to mention here that in November 2001 the Council of Europe signed a 'Convention on Cybercrime'; cyber crime is just one more aspect to take into account, even if not one of the most important ones, in relation to national and international security.

In recent years, however, some European countries, including Germany, The Netherlands, Norway, Sweden, Switzerland, and the UK, have started initiatives on vulnerabilities analyses of their infrastructures, a sketch of early warning systems, in some cases also suggesting countermeasures and setting policies within this framework. Austria, Finland, France, and Italy are also becoming increasingly active in this domain.

The United Nations (UN) also recognised the importance of this issue. In December 1998, the General Assembly released Resolution 53/70, addressing the security of global information and telecommunication systems and promoting the consideration of existing and potential threats in the field of information security. In 1999, two UN agencies – the Department of Disarmament Affairs (DDA) and the Institute for Disarmament Research (UNIDIR) – organized a discussion meeting on 'Developments in the field of information and telecommunications in the context of international security'. If we exclude bilateral and multilateral contacts, this was the first meeting on this topic to be held within the UN community. In December 1999, a second Resolution (54/49), collecting the views and assessments of a certain number of countries, invited member states to define basic notions related to information security and the development of international principles in order to enhance the security of global information and telecommunications systems. Since then, further resolutions have been adopted by the General Assembly (55/28, 56/19, 57/53, 58/199), indicating the increasing interest around this topic within the UN.

3.3 Critical infrastructures

What exactly do we mean by the term 'infrastructure' in this context, and why does it need protection? An infrastructure is a framework of interdependent networks and systems, generally interlinked at many different levels, including industries, institutions and distribution capabilities that provide a flow of products or services. Some infrastructures are becoming essential, if they are not already, for the organization, the functionality and economic stability of a modern developed country. To be more specific, it is possible to identify five main sectors (following the scheme of the report entitled 'Critical Foundations', released by the PCCIP Commission), each one including very broad domains:

1. Information and communication.
2. Energy.
3. Banking and finance.
4. Physical distribution.
5. Vital human services.

This section will address each of these items in turn. The 'Critical Foundations' Report will be referred to as the 'PCCIP report'. One should not forget, however, that this is just one of many possible schemes to describe and analyse the complexity of the problem; different approaches are possible, in terms of components, networks, services and domains. These infrastructures are considered 'critical' in the sense that they are supposed to be indispensable for normal day-to-day civil life and their incapacitation or destruction would have a debilitating impact on economic security or the defence capabilities of a country. It is worth pointing out that these five sectors are not independent, but very strongly correlated to one another. What follows is a very concise description of the critical infrastructures included in each of the five sectors.

The *Information and communication* sector includes all the telecommunication equipments, the computer and network technologies and techniques (both hardware and software), the lines providing connectivity and Internet-based services. It includes the Public Switched Telephone Networks (PSTN) providing voice, data, video connectivity and private lines, in addition to the millions of computers used for commercial, academic and government use and in private homes. This sector includes the support for processing, storage and transmission of data and information, including the data and information themselves. Currently, we are witnessing a global merging of all of these infrastructures.

The complex systems of production, storage and distribution of every form of energy characterizes the *Energy* domain: natural gas, crude and refined petroleum, nuclear power, including processing facilities, and electricity. For example, the electrical power grid of a country is part of this infrastructure; this domain also fuels the transportation services, manufacturing operations and home utilities, and is essential to many other infrastructures. It is a key component to other infrastructures and vital for the economic stability of a country.

The *Banking and finance* sector includes entities such as banks, commercial organizations, investment institutions, trading houses and associated operational organizations and support activities like financial transaction services, electronic payments and related messaging systems. To give an example, in the USA this infrastructure manages trillions of dollars – from individual deposits and pay cheques, to transfers for major global enterprises.

The networks of roads and highways, railways and the airspace system (airlines, aircraft and airports) characterize the *Physical distribution* sector, which also includes national pipelines, ports and waterways. This infrastructure allows the movement of goods and people within and beyond the borders of a country.

Finally, the *Vital human services* sector includes emergency services (for example, police, fire-fighting and rescue services), government services, state and local agencies, and country-wide water supply systems serving, among others, agriculture, industries and homes.

The mosaic of interconnectivity makes the global infrastructure extremely complex. It is extremely difficult to define and establish exact boundaries, measure impacts of events and identify clear responsibilities for the management of the different frameworks. It should be noted that two infrastructures – the 'Energy' sector (in particular the distribution of electric power) and the 'Information and communication' sector – underpin the other infrastructures, so that the interruption or disruption of these sectors could potentially have the widest effect. The current trend is that all the critical infrastructures are increasingly dependent on ICTs.

In addition to natural disasters, failures and human misbehaviour, each of these infrastructures, depending on its design, implementation or operation, can be susceptible to destruction or incapacitation and is vulnerable to some extent. This vulnerability can be at the physical level, at the cyber level, or at any combination of the two; this combination, in particular the cyber physical dependence, is the most obscure sector. The problem arising at the beginning of the Year 2000 from the incorrect handling of a two-digit year date format in many application programmes, the well-known 'Y2K bug', can be considered to be an example of this. The attention paid in estimating the possible consequences produced by Y2K, in particular by western countries, shows that already it is difficult to assess the effects of a single software bug, relatively simple and not malicious, distributed over many systems spread over our basic information infrastructures. Even if the Y2K problem might have been overstated for commercial reasons or by the media, it is a fact that users, and sometimes not only end-users but also professionals, are not fully aware of all the low-level detailed features (not to mention real software bugs) within each application and, most importantly, all of the indirect consequences of these 'features', especially in complex systems. This problem is particularly evident in the security domain.

3.4 Vulnerabilities

What are examples of possible vulnerabilities within the various domains? 'Energy' and 'Physical distribution', in particular, may suffer physical vulnerabilities to various degrees, caused, for instance, by natural disasters or sabotage, but here we wish to focus on possible problems and threats of a different nature.

Information and communications: in addition to natural disasters, the primary threats to this sector are system failures and instabilities arising from the increased volume and complexity of interconnections. In the past there have been documented deliberate attacks and intrusions through the software-based disruption of network devices and management systems. In recent years PSTN has become increasingly software driven, remotely maintained and managed through computer networks, which has increased the possibilities of electronic intrusion. The existence of mega-centres for operations support creates single points of failure and makes the targeting of hostile actions easier. The infrastructure vulnerability has probably grown during the 1990s; as far as the Internet is concerned, high-level security was not a primary design consideration during its evolution and deployment.

Energy: the level of vulnerability of this sector has been increased by the recent rapid proliferation of industry-wide information systems based on the open architectures used in the operating environment. This includes increasing reliance on communication links, which sometimes runover public telecommunication networks. As a particular example, the widespread and expanding use of the Supervisory Control and Data Acquisition systems (SCADA) to monitor and control energy infrastructures, runs the risk of serious damage and disruption by cyber means. SCADA is employed by the electric power, oil and gas industries. Possible electronic intrusion through public networks could cause significant disruption if an intruder were able to access the system, modifying the data used for operational decisions or taking control of procedures for critical equipment. Dangers also come from the extended use of commercial off-the-shelf (COTS) hardware and software. COTS are considered risky because detailed specifications might not be available or may simply not be met by some of the components, causing limitation of functionality or faults because of the presence of lower quality standards; they sometimes have built-in vulnerabilities and may pose problems of security and dependability. In addition, sometimes vulnerability information, useful for the targeting of traditional military activities, is made publicly available.

Banking and finance: this is considered the safest domain, and the main vulnerabilities are of a physical nature. Strong measures have been taken, especially in the USA, to harden primary facilities, to secure the infrastructure and to provide extensive system redundancy; however, there remains some level of risk from the disruption of telecommunications and electric power services. In addition to large-scale infrastructure vulnerabilities, this area suffers because of significant opportunities for theft and fraud in individual institutions. Insiders, who might use authorized access to collect confidential information or operate systems for personal profit, constitute the most persistent security threat. Due to its intrinsic sensitivity and in order to maintain public confidence, financial institutions will often refuse to use external agencies in problem reporting, reducing the transparency of the system and making the discovery of intrusions and the protection of the overall infrastructure sometimes more complicated.

Physical distribution: as in other areas, cyber vulnerabilities are emerging, as this sector relies increasingly on IT and communications infrastructures. Every aspect of the transportation industry is affected – for example, the rapidly expanding use of Intelligent Transportation Systems to optimize and increase overall efficiency. In some cases, data publicly available on the Internet could be used to collect information on potential military targets.

The PCCIP report states that, in the USA, the most significant projected vulnerabilities are considered to be those associated with the modernization of the National Airspace System (NAS) for air traffic control. This includes plans to adopt the Global Positioning System (GPS) as the sole basis for radio navigation in the country by 2010. At present, NAS is relatively immune from intrusions, being composed of difficult-to-penetrate dedicated subsystems and networks. The newly planned architecture is likely to use open systems and shared communications networks in conjunction with COTS hardware and software products. As a consequence, the risk of unauthorized access and the probability of malicious actions would increase substantially. As far as GPS is concerned, current plans could lead to overreliance on this system, which is vulnerable to jamming (transmission of noise interfering with original signal) and spoofing (broadcast of false GPS information).

Vital human services: in this sector the main concern in relation to cyber vulnerabilities is probably the increasing reliance on SCADA systems being used for the control of water supplies; in addition, some emergency systems can be overloaded through misuse. Government services keep mega-databases containing highly confidential information on private citizens; cyber intrusion into these databases is a concern as is, once again, the general dependency on computer technology. In addition, cyber reconnaissance to track military assets might be possible in some cases.

More detailed examples can be provided: the first one concerns PSTN, where the level of vulnerability is growing. In recent times, the number of interconnections among telephone companies has increased, including, in particular, interconnections through the Internet. This means that two different telephone networks, using SS7 (Common Channel Signalling System 7, known also as C7) standards, can be interconnected through an Internet Protocol (IP) packet network like the Internet. In other words, a phone call can be transmitted from the caller's local switching point to a 'SS7-IP gateway', travel through an IP network to a second gateway where it re-enters a different telephone network in order to reach its final destination. SS7 is a global open standard defined by the International Telecommunication Union; it describes procedures and protocols by which PSTN network elements exchange information over a digital signalling network for call set-up, routing and control. SS7 was originally designed for a closed community of telephone companies, but recently there has been a proliferation of new services and a significant increase in the number of SS7 vendors providing both hardware and software products. This trend necessarily induces a relatively high level of information sharing and standardization, increasing the overall vulnerability of the global system; many more actors are now present on the scene, a situation that is creating opportunities for insider attacks. The main point to stress here is the relatively recent interconnection between the traditional telephone systems and digital data network: the IP 'trunk' is relatively easier to intercept than the traditional SS7 traffic. In some cases, existing SS7 firewalls might not be adequate or reliable enough, allowing external IP packets, injected into the Internet in the proper format, to enter the telephone network through the SS7–IP gateway. More generally, leaving aside SS7, many present switchboard systems can be remotely managed through their network connections and are built on top of computers running standard operating systems, with known vulnerabilities. Among possible consequences of an intrusion are unauthorized call control or modification of call routing tables within the telephone exchanges.

Another example of vulnerability is the transport architecture of switched networks. As mentioned also by the PCCIP report, many of the fibre optic network installations by commercial carriers are configured as Synchronous Optical NETworks (SONET), a standard for physical-level transport, supporting Asynchronous Transfer Mode (ATM) based services, present at the network backbone level. In SONET most of the elements are remotely managed through packet data network connections, which are somewhat vulnerable to electronic intrusions; in addition, the maintenance and testing ports of network devices could be remotely attacked. Even if it might be less relevant these days because of changing technologies, in the past this was the cause of a large-scale network outage produced by a cyber attack.

One more example concerns emergency systems; in April 2000 NIPC released an alert on a 'Self-Propagating 911 Script', spreading through four of the major US Internet service providers where thousands of computers were scanned for disseminating the malicious script. Victim systems would dial 911, an emergency phone number in the USA, causing authorities to check out substantial numbers of false calls and overloading the infrastructure.

Coordinated Distributed Denial of Service (DDoS) attacks (where servers are flooded by a number of request messages they cannot cope with, originating from multiple locations on the Internet) in some cases produced real and substantial financial loss. This was the case in February 2000, when a number of high-profile attacks temporarily disabled some important electronic commerce Internet websites; sophisticated DDoS tools appear to be undergoing active development, testing and deployment over the net. Recent relatively sophisticated attacks appear to have been planned for weeks or months, since they require clandestine loading of hacking software onto hundreds of computers around the world.

In the previous section SCADA systems have been mentioned; together with DCS (Distributed Control Systems), they are part of the larger class of industrial control systems, often used for operation and maintenance of critical infrastructures. These systems, used for data acquisition (through monitoring sensors) and control (through actuators), perform key functions in providing essential services for electricity generation and distribution, for the water supply infrastructure, waste treatment systems and oil and gas industries. These control networks were initially designed to optimize functionality, but they paid little attention to security which, in many cases, could be considered weak or non-existent; in the past, this was not a problem since systems were completely decoupled from any other network and were basically accessible only by authorized operators on dedicated infrastructures. Basically, old architecture was not designed for the current transition from the 'analogue' to the 'digital' world. More recent control systems using SCADA rely heavily on digital information technologies, using standard software tools, operating systems and communication protocols; in some cases, the control system is interlinked with other general purpose network and is being operated in a way for which it was never designed. As a consequence, new control systems inherit vulnerabilities from the IT sector and become prone to cyber-based attacks. Often there are inadequate password policies, there is no protection against data interception or manipulation, commercial operating systems and communication protocols have known weaknesses and often there is no protection against spoofing in the underlying low-level communications. Some logic controllers could even crash (thereby losing control of the device) under a simple remote port scan; and viruses and worms could probably be specifically designed to target SCADA infrastructures.

3.5 Actors: how and who

The examples in the previous section show how the basic communication infrastructure, including both the telephone and Internet networks, can be vulnerable under certain conditions; it is important to point out that other sectors rely on them for their normal day-to-day activities. All of the critical infrastructures are increasingly interconnected through communication networks. This relatively recent trend increases global efficiency but, as a side-effect, it decreases resilience; it is recognised that mutual dependence and interconnectivity bring new vulnerabilities. The management of complex interconnected systems is a difficult task, especially because of their interdependencies. From the security point of view, the risk lies at different levels, ranging from generic crimes like frauds or criminal activities using the net, to sabotage, interception and intrusion. The spectrum of targets is also very broad, from individuals to institutions. Restricting discussion to the IT sector only, the possibilities of break-ins and hacking are high at the user, computer, and network levels. Various sorts of 'Hacker Kits' are freely available on the Internet; the tools are so numerous and so varied (and often sophisticated) that some kind of zoological approach would be needed to classify them. For example, it is possible to map the network topology using 'scanner' programmes and intercept and look at the content of packets travelling through the data lines using 'sniffer' applications. It is possible to hack or poison the ‘Domain Name Service’ (DNS, a basic functionality translating IP addresses into computer names) or produce broadcast storms that may drastically reduce network availability. Under certain conditions one can remotely crash or shut down computers or network devices or limit some of their functionality. In order to gain access to computer systems, it is possible to use password cracker programs or exploit ‘buffer overflows’, executing code in reserved and unprotected memory space. To this list of dangers we can add Trojan horses (disguised malicious applications), viruses (self-reproducing code attached to executable code) or worms (autonomously transferring replicas of themselves over the network). In general, there are two main phases in mounting an IW attack: the first step is to perform a detailed mapping of the net, collecting data on active network devices to carry out a vulnerability analysis. In this respect, many networks worldwide detect a more or less regular activity of mapping, often performed by unidentified sources. In the second phase, the appropriate software weapon is released. Release does not mean activate; the activation can come later, programmed to occur at a certain time, under defined, logical conditions or following a specific command. In some cases a test reaction can be performed in advance, to ascertain the defence capabilities of the attacked system.

Who are the actors involved in such activities? Here again the spectrum is very wide; with no intent of being exhaustive, it is possible to distinguish a few general classes. Media like TV or newspapers often refer to generic ‘hackers’, who can be professionals or, more often, amateurs or hobbyists, people who like spending nights in front of a computer screen breaking into electronic systems. They often have no explicit malevolent intent, but view their activities as a personal challenge. A second group includes insiders, who are often involved in cases of industrial, economic or corporate espionage; this group is often motivated by money or revenge and can pose a significant threat for organizations. The third group consists of criminals at the individual level or within organizations, targeting, for example, financial information resources. Corporations actively seeking competitors’ trade secrets, often using insiders, can fall in this category. Furthermore, there are politically motivated state and non-state groups, ranging from government agencies like intelligence agencies or military units to terrorist groups; their goals can include information collection, propaganda, electronic surveillance, censorship and sabotage.

Concerning the resources required for such an activity, it should be pointed out that even if the entry cost of micro-computing and networking devices is relatively low (a simple, cheap, PC with a modem can be sufficient to annoy system administrators), in order to become a meaningful actor in this context a fair amount of intelligence gathering is needed, together with a high degree of technical expertise and the availability of a large amount of resources.

3.6 Open questions and comments

Before making some general comments, let us refer once again to the PCCIP report of October 1997 and summarize the USA's strategic objectives as set out in this document. This report recognises that the technological dependence on critical infrastructures is increasing and that there is a widespread capability to exploit infrastructure vulnerabilities. It also states that in society, there is insufficient awareness of this topic and it suggests various actions to be taken by the government. First, the problem needs to be defined more precisely. A systematic examination and a very detailed evaluation of critical infrastructures have to be performed in order to propose a precise strategy to protect them. The interconnectivity among different systems has to be analysed in detail, together with the cyber/physical interdependency, to assess the level of vulnerability; the complexity of the problem has to be addressed and the current level of protection and risks understood. The second logical step is to gather information from the government and infrastructure owners and operators, for example, telephone companies and network providers, so that there can be some understanding of who exactly controls which sectors. In addition, it needs to be clarified where responsibilities lie – if they are public, private or shared – in order to understand who is supposed to take action. It suggests starting a close public–private coordination and cooperation between government and industries, promoting a partnership to accomplish their specific infrastructure protection roles. The government should take the leadership in information security management activities, promote inter-agency coordination and integration, and sponsor legislation to develop the legal framework in order to increase the effectiveness of protection efforts. The national awareness of infrastructure vulnerabilities and threats should be raised through education and other appropriate programmes. At the beginning of the Year 2000, the US president began addressing this subject in public speeches. In order to protect infrastructures, the PCCIP report proposed the creation of a national cyber-warning capability, providing immediate real-time detection of attempted cyber attacks on critical infrastructures; the goal is to monitor, provide early warning, alert and respond in order to reconstitute a working minimal infrastructure even with limited functionality. The report also recommends increasing investment in infrastructure assurance research and design (R&D) from $250 million to $500 million in 1999, with incremental increases over a five-year period to $1 billion in 2004. This is an extremely brief summary of the views of the PCCIP Commission; the full document contains very interesting details. Different views exist on the subject, however, the appointed governmental commission made a significant contribution to producing the report and hence it cannot be underestimated.

In January 2000 the White House released the 'National Plan for Information Systems Protection', an attempt to design a way to protect cyberspace;

it can be considered as the evolution of the PCCIP report, which is clearly the starting point. This plan follows very precisely the strategic views of the 1997 report and contains technical R&D and training programmes. In addition, it supports activities to increase public awareness, but also to ensure the protection of civil liberties and protection of proprietary data. A public–private partnership is strongly encouraged to build the base for cyber defence. This plan was supposed to be fully operational by mid-2003; the current US administration seems to share basically the same views on the argument. Apart from the US, a few more countries are currently in the first steps of a detailed analysis of their infrastructures, addressing interdependencies and vulnerabilities.

In spite of all this activity, these are several open questions and some important unresolved issues. In the following, some topics will be briefly discussed, but many more details and analyses can be found in the reference at the end of this chapter, to which the reader is directed. The first issue is about information sharing between public and private sectors: it is evident that in order to reach the goal of centralized analysis and monitoring there is a compelling need for information sharing, up to some non-negligible level, between the two sectors. This sharing can be problematic for various reasons, mainly because of the sensitivity of shared information and the possibly divergent interests of the actors. Security agencies are usually reluctant to release confidential and classified information, while industries in competition in the market would like to retain trade secrets and proprietary information. The situation is made even more complicated if we take into account multinational or foreign corporations. The responsibilities of government and private sector may be conflicting and interests may diverge; an example that occurred in the past was the dispute over encryption between a US citizen and the Department of State. Another topic for debate is the following: what exactly is the government's responsibility? Defence of the country has always been the exclusive preserve of the government, but this may no longer be either true or even feasible, since the civilian sector may no longer be fully protected by interposing military forces. In addition, in the new scenario, private owners and infrastructure operators need to play key roles in infrastructure protection against intrusion, frauds or possible foreign attacks. Where to draw the line between public and private sector responsibility? Can it be drawn at all, or is it becoming fuzzy? A close collaboration between citizens and national security agencies might drive us towards a surveillance society.

The issue becomes more complicated because of the economic deregulation process currently underway, which is causing a higher level of infrastructure vulnerability. The growing fragmentation of systems reduces the control of each individual operator, often limiting redundancy and increasing the overall level of fragility. In the telecommunications sector especially, the appearance of new multiple intermediaries into what were once end-to-end services makes the level of operational interdependence even more complex. As a consequence, the management and coordination of complex systems becomes more and more difficult. The PCCIP report and the national plan suggest and support R&D activities on topics like intrusion monitoring and detection and incident response and recovery. As we mentioned above it also plans to create a national cyber-warning capability. It is interesting here to go into more detail: it implies the capacity for near real-time monitoring of telecommunications infrastructures, the ability to recognise, collect and profile anomalies associated with attacks and, finally, the capability to trace, re-route and isolate the electronic signals associated with an attack. The complexity of the overall system, which is also constantly changing, makes tactical warning and attack assessment an extremely difficult problem. Distinguishing between the 'noise level' of day-to-day accidental events and real attacks and, in addition, being able to trace the source of an attack might be a formidable task. On this subject, it is worth saying that intrusion monitoring applications and products are being built and commercialized by the computer and network industry. The risk of evolving towards a surveillance society might be even higher if legislation is not correctly set up to avoid the misuse of such facilities. In the USA, for example, the conflict could be with the 'Fourth Amendment', protecting individual privacy from unwarranted governmental intrusion. It is appropriate to mention possible legislative conflicts and jurisdictional controversies, a new area on which a public debate would be very interesting. One can ask himself the question whether, in addition to defensive tools and techniques, some actors are actively building offensive info-war capabilities. The boundary between national and international security might become thinner and thinner, like the distinction between military and civil sectors.

3.7 Conclusions

The PCCIP Commission found 'no evidence of an impending cyber attack, which could have a debilitating effect on critical infrastructures' (so no imminent threat had been observed at that time), but a 'widespread capability to exploit infrastructure vulnerability'. As in many other debates, there are radical voices; those who think that hackers are on the verge of destroying basic infrastructures in developed countries. There are also sceptical voices who think that the whole argument is just information mania, and that the catastrophic scenario view is just for 'demo' purposes in order to absorb the vast amount of money made available by the US government to prevent something hypothetical from occurring. The scenario that has been drawn in the previous sections is very complex and this complexity has not been hidden in order to give the reader a feeling of the overall picture. This chapter is intended to be an introduction to the subject so, in order to limit its length, many arguments have been only briefly mentioned and oversimplified, a few have been skipped. In order to disentangle the complexity we will try to focus on some facts in an attempt to summarize the key elements.

Given the recent and ongoing digitalization of industrialized countries, it is evident that critical infrastructures exhibit a growing dependence on networked information systems and communication technologies; this dependence is a source of vulnerability at many levels. Widespread reliance on information-based technologies has resulted in an unprecedented degree of global connectivity and interdependence, making overall management more complex and causing possible disruptions and cascading effects, as in a chain reaction. In addition, from the point of view of security, the superposition and the current process of merging traditional critical infrastructures and information infrastructures increases the global vulnerability, induced by electronic attacks, which was, up to now, limited only to the IT sector.

In the medium term, the development of sophisticated tools and more robust systems might reduce this vulnerability, let's hope this will happen, this is the direction efforts are going. At the moment it is evident that cyber attacks are technically feasible at different levels of complexity. They are not only feasible, but take place all the time in the worldwide networks; the consequences, often not only of economic nature, are difficult to estimate.

It is evident to any computer or network security expert that IT infrastructures can be highly vulnerable – at least locally – to a limited scope attack; small-scale or temporary disruptions can be relatively easy to produce. On a larger scale, it is quite difficult to assess the level of risk and the associated vulnerability. Evaluating the effects of the interconnection and interoperation of very different systems and infrastructures can be an extremely complicated task; only now are we learning how to master systems at such a level of complexity.

Possible military and intelligence activities, with both defensive and offensive roles, cannot be excluded in this context; on the contrary, some countries are explicitly addressing them. The exploitation of advanced IT is driving what some people describe as the Revolution in Military Affairs (RMA). Some countries are probably analysing the possible impacts of a potential enemy's information infrastructure disruption. Obviously, national security is of primary importance for every country in the world, but this has to be balanced with the right to privacy and the security of personal and commercial information in a worldwide domain, and, of course, with the national security of other countries. Given the transnational nature of the problem, clear international principles need to be established and agreed upon in order to enhance the security of global information and telecommunications systems. UN resolutions adopted by the General Assembly recognise the need to define notions to deal with unauthorized interference, or the misuse of information systems and resources. For example, appropriate bodies (the United Nations, the International Court of Justice, the G8, bi- and multilateral negotiations or other agencies) might be chosen for dealing with non-peaceful purposes of ICT. The very nature of global networks goes beyond the jurisdictional limits of each country, so an adequate legal framework to develop a uniform legislation is required, as long as there is a clear definition of a chain of responsibilities among the different actors. International cooperation at various levels should be fostered. Some initiatives show that military and civilian activities and functions tend to merge; IT can be considered to be an example of dual-use technology. After all, many scientific and technical developments have had, and continue to have, both civilian and military applications. Cyber development of military affairs is well underway; the 'information weapon' might not be only a virtual concept. The evolution of this field, recognising the broadest positive opportunities, should also be followed in the context of international security, in order to prevent the potential misuse of these technologies for criminal purposes and to avoid undermining international stability.

References

Centre for International Security and Arms Control, *Workshop on Protecting and Assuring Critical National Infrastructure: Next Step* (Stanford, CA: Stanford University, 1998).

Chapman, G. 'National Security and the Internet', paper presented at the Annual Convention of the Internet Society, Geneva, 1998.

Denning, D.E. *Information Warfare and Security* (Boston: Addison Wesley, 1999).

Joint Economic Committee US Congress, 'Security in the Information Age: New Challenges, New Strategies', *Report of the Joint Economic Committee US Congress* (USA, 2002).

McClure, S.J. Scambray and G. Kurtz, *Hacking Exposed* (California: Osborne McGraw-Hill, 1999).

Molander, R. S. Riddile and P. Wilson, *Strategic Information Warfare: A New Face of War* (Washington RAND: MR-661-OSD, 1996).

Neumann, P.G. *Computer Related Risks* (Boston: Addison Wesley Professional, ACM Press, 1995).

Northcutt, S.J. Novak and D. McLachlan, *Network Intrusion Detection: An Analyst's Handbook*, 2nd edn (USA: New Riders Publishing, 2000).

President's Critical Infrastructure Protection Board, The National Strategy to Secure Cyberspace, *Report of the President's Critical Infrastructure Protection Board* (USA, 2002).

Rathmell, A. 'Cyber-Terrorism: The Shape of Future Conflict?', *Royal United Service Institute Journal*, (October 1997).

Siroli, G.P. 'Strategic Information Warfare', *Research Paper 2001/2, Geneva International Peace Research Institute (GIPRI)*, (2001).

Sun Tzu Ping Fa, and R.D. Sawyer, *The Art of War: Sun-Tzu Ping Fa* (Boulder, CO: Westview Press: 1994).

Tanenbaum, A.S. *Computer Networks* (USA: Prentice-Hall International, 1998).

The Report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (October 1997).

The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection* (January 2000).

UN General Assembly Resolutions: A/RES/53/70 1998, A/RES/54/49 1999, A/RES/55/28 2000, A/RES/56/19 2001, A/RES/57/53 2002, A/RES/58/199 2004.

Ware, W.H. *The Cyber-Posture of the National Information Infrastructure* (Washington: RAND, 1998).

Dunn M. and I. Wigert (A. Wenger and J. Metzger (eds), *International CIIP Handbook 2004: An Inventory and Analysis of Protection Policies in Fourteen Countries* (Zurich: Center for Security Studies, 2004).