Critical Infrastructure Protection: Survey of World-Wide Activities

Abstract
Critical Infrastructures (CI), such as telecommunications, power supply and transport, fulfil essential functions in modern states. If any failure should occur in these vital services or if essential elements of infrastructure should break down, the impact could spread to other sectors as well because of interdependencies. In today’s networked world, it is possible for serious damage to extend beyond national frontiers and harm other states as well. Infrastructure protection has therefore become a global challenge that needs to be addressed. Today no state can close its eyes to the need for continual review and improvement of infrastructure protection. However, the definitions of critical infrastructures in different countries are as diverse as the concepts of infrastructure protection that have been developed in those countries: whereas it may be possible to identify some common structural elements between countries, the measures taken so far, the functions performed by the organisations responsible for infrastructure protection and the degree of protection achieved to date differ widely.

Structure of Critical Infrastructure Protection
There are two universal statements that can be made regarding the protection of critical infrastructures all over the world: it is simply not possible to achieve 100% security of critical infrastructures in any country and there is no single ideal way of tackling the problem. But although in every country the approaches adopted are heterogeneous, nevertheless three main categories can be identified.

The first of these is the Critical Information Infrastructure Protection (CIIP) approach. Content-wise, this refers exclusively to the security and protection of the IT connections and IT solutions within and between the individual infrastructure sectors. Protection of the physical components is ensured in a separate organisational framework. Functions and competencies relating to critical infrastructure protection (CIP) are spread between different organs. Moreover, an attempt is made to integrate the private sector at all levels of CIP.

The second approach entails both the protection of critical IT infrastructures and also the physical protection of critical infrastructures. Here, physical protection is part of the national civil defence model and the central co-ordination and strategy organs are simultaneously centres of competence in IT security, civil defence and disaster control. There is no clear separation between the individual components. Moreover, the prominent role of national ministries of defence, due to their co-ordinating role, must be stressed. The authors call this approach the All Hazards approach.

---

1 This paper is based on a study that was carried out by Jörn Brömmelhörster, Sandra Fabry and Nico Wirtz for the BSI, and provides a summary of that study. Over 20 countries/organisations and the organisations responsible for critical infrastructure in those countries were selected for the study. The selection criteria were the significance and status of the relevant approach to critical infrastructure protection (CIP) and the accessibility of related information. The individual approaches to infrastructure protection were evaluated solely according to criteria devised by the authors. The investigation focused on the form of infrastructure protection strategies rather than on the technical measures adopted in each case, and relied entirely on material available in the public domain up to September 2002.
Both approaches attempt to integrate both state and private players into the national organisational model, but co-operation between the public and private sectors at the strategic planning level is often totally absent or else only of a rudimentary nature.

The third approach is a special case, as the only instance of this is the Chinese model. Here there is no co-operation between the public and private sectors. The model serves less to protect the national critical infrastructures than to preserve the system of government and the organs that represent the interests of the state.

One of the yardsticks against which one can evaluate the approaches of different countries is the question of whether a national, compelling strategy for critical infrastructure protection (CIP) exists or not. This the study authors believe exists only in approaches in the USA and is totally absent in all other countries.

In this context they refer to the absence of clear definitions as to what needs to be achieved in the area of national critical infrastructure protection. They also stress the fact that functions and competencies are seldom clearly delineated and localised. The fact that most countries are not carrying out any independent, national threat analysis is viewed as another shortcoming. Frequently the American perception of the threat is adopted without modification, and the authors attribute to the USA a pioneering role in virtually every area of CIP. Here they point out that all the other states are in fact trying to match their approaches to those of the USA, without adequately taking country-specific differences into consideration. Often in these countries the only analysis undertaken is of dependencies and interdependencies; asset analysis programmes are otherwise confined solely to the public sector.

The authors believe that inclusion of the private sector is imperative. They emphasise that approx. 90% of national critical infrastructures are actually in the hands of the private sector. Moreover, they believe that the companies in the private sector are best placed to assess what systems and subsystems within their own business or sector require special protection. They therefore call for greater co-operation and point out the importance of strategic controlling, i.e. the merging together of the individual elements involved in critical infrastructure protection. Countries that have adopted the All Hazards approach are viewed as being particular weak as regards co-operation with the private sector.

Another aspect relevant to consideration of the private sector is the degree of organisation and co-operation. Whereas in the USA this is relatively well established thanks to the Information Sharing Analysis Centers (ISACs), such organisational forms are virtually absent in other countries or else they are copied with minimal tailoring to country-specific circumstances. However, the authors refer to difficulties regarding the establishment and efficiency of ISACs.

Again, the authors believe that fundamental questions regarding the division of competencies and functions and also information, co-operation and reporting procedures have not yet been adequately clarified. Particularly in countries that have adopted the CIIP approach, overlaps are frequently found along with inadequate delineation of areas of responsibility.

The transparency\(^2\) of the national system for the protection of a state’s own critical infrastructures is viewed as vitally important. It is essential to the attainment of adequate critical infrastructure protection that proper awareness of the problem is created at all levels of industry, state and society. When it comes to information campaigns, the USA and the Netherlands are the clear leaders. In countries that have adopted the All Hazards approach, the most significant shortcomings result from the prominent role played by the national ministry of defence.

In summary, the authors point out that it is a mistake to assume that the threat situation is the same in every country and that a single, large-scale, global strategy is all that is required.

---

\(^2\) Availability of freely accessible information
They note that every country is only at an elementary stage as regards the protection of their critical infrastructures. There is a massive need for action here. They believe it is especially important that national critical infrastructure protection should not be confined to the public sector and that it should not stop at the national frontiers either. International co-operation to date has been of only a rudimentary nature and must be stepped up as a matter of urgency.

Country Overview

**USA**

The USA has made a lot of progress, relatively-speaking, as regards a strategic architecture for critical infrastructures and their protection. Access to resources has been virtually unfettered since 11 September, and many organisations in the USA are concerned with critical infrastructures. In the meantime, the objective of achieving all-embracing critical infrastructure protection by 2003 has been set aside.

The Department of Homeland Security (DHS) is now co-ordinating all the US government’s critical infrastructure protection initiatives at governmental level and has incorporated a number of different governmental agencies. This should help to unify responsibilities in the USA in the CIP area and thus avoid the situation where similar programmes are initiated by more than one agency. Co-operation with the private sector is working, and the idea of creating Information Sharing Analysis Centers (ISACs) originated in the USA. The American system can now be described as transparent. Since the events of 11 September 2001 critical infrastructure protection has become a top priority.

**Canada**

Canada has incorporated information and communication technology (ICT) protection into its “Total Defence” overall concept and follows the All Hazards approach. An attempt has been made to transfer as many critical infrastructure protection functions to existing civil defence organisations. The Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) has taken over the function of national strategy and co-ordination organ. The Canadian Department of National Defence plays a prominent role in the matter of critical infrastructure protection. There is no separation between military and civilian areas. The individual agencies are themselves responsible for implementing IT security measures on the basis of the Government Security Policy. Up to now there has been little involvement of the private sector. There is an absence of institutionalised mechanisms for the exchange of information and for co-operation between public and private organisations. So far duplication of programmes has been avoided. To date there has been little in the way of public information programmes in Canada.

**The United Kingdom**

Until the end of the 1990s critical infrastructure protection was not a concern at the highest level. In the last few years functions and competencies relating to the protection of the national critical infrastructures have been transferred to existing organisations; there is no strategic overall concept. The critical organs are the National Infrastructure Security Coordination Centre (NISCC) on the state side and the Information Assurance Advisory Council (IAAC), a public-private forum. Parallels with the USA must not be overlooked. The question of ultimate responsibility has not yet been clarified in the United Kingdom. Moreover, neither in the public nor in the private sector is there any programme for examining the criticality of individual systems. Bringing together those with responsibility for critical infrastructure protection (CESG, MI5, the police, the Ministry of Defence) in the NISCC’s management board means that an organ exists for the exchange of information which can then be merged into a national overall picture by the NISCC. Since the establishment of the Government Liaison Panel in 2001, the private sector has been integrated into the national structure. Nevertheless, most programmes are still geared up towards the public sector. The British model can

3 Updated for this paper.
only be viewed as transparent up to a point. There is a total absence of any virtual information campaigns.

The Netherlands
The initiative to protect the national critical infrastructures originated in the Dutch ministry of defence. The state’s role as regards critical infrastructure protection (CIP) is simply to prescribe a national strategy, modify the legal situation to the new threats and promote innovative ideas in the ICT area. All functions at tactical and operating level are either viewed as a function shared between the public and private sectors or else are assigned explicitly to the private sector. In the view of the Dutch, every critical infrastructure sector / every ICT user bears responsibility for its own critical infrastructures. Under the Dutch model, the private sector plays a particularly important role and there is no central state organisation that coordinates and controls national CIP measures. This function is performed by the private organisation, *Electronic, Commerce, Platform Netherlands* (ECP.NL). The government’s policy document *VIR 1994* sets out the framework for IT security for the public sector. In the private sector there are still major problems as regards co-ordination and co-operation on issues that are directly relevant to security. So far duplication of structures has not been eradicated.

Switzerland
The Strategic Management Exercise of 1997 resulted in adoption of the “Strategy for Information Society Switzerland”. Since then the Swiss ministry of defence has played an important role in the CIP area. In Switzerland, critical infrastructure protection is mainly understood as military-political and state function. To date there has been no real integration of the private sector, and co-operation is confined to areas that are viewed as necessary to safeguard civil defence functions. Moreover, under the Swiss model, there is no organisation that can function as central (national) control and co-ordination organ. The most important organisation is the *Swiss Department for Defence, Civil Defence and Sport*, which looks after all the main CIP programmes. There are plans to set up a central information security reporting and analysis office (MELANI). Duplication of structures has been avoided in Switzerland and it is hoped to further integrate the private sector.

Sweden
Under Sweden’s “Total Defence” approach, critical infrastructure protection has been integrated into the general complex of national defence. Critical infrastructure protection is viewed as a combination of information assurance, critical infrastructure protection, defensive information operations and defensive information warfare. The private sector has successfully been integrated into the organisational construct at the essential levels, but nevertheless the position of the ministry of defence remains exposed. The question of ultimate responsibility has been clearly defined, as have the management and leadership functions for the central organs of the *Swedish Emergency Management Agency* (SEMA), the *Technical Competence Centre* (TCC) and GovCert. All the relevant players in the public sector are involved in SEMA. In the private sector, CIP measures are proceeding in a totally uncoordinated fashion, and there is no co-ordinating organ. Compared with the high degree of organisation at the level of the public sector, there is no comparable model on the side of the private sector. Duplication of structures has deliberately been avoided in Sweden, but much remains to be desired in the area of education. Nevertheless, the Swedish model can be described as transparent.

Australia
The Australian model is based on consultation and co-operation, even if in the public sector methodical implementation has been left in the hands of government agencies. The leading bodies involved in formulating a strategy on critical infrastructure protection (CIP) are the public sector consultative organs, *E-Security Coordination Group* (ESCG) and the *Critical Infrastructure Protection Group* (CIPG). Establishment of the *Business-Government Task Force* in 2001 was a significant step in the direction of integrating the private sector into stra...
strategic planning for CIP. On the other hand, most programmes and functions in the national model are confined to the public sector. The exception to this is AusCERT, which makes its services available to the private sector independently. The Australian model can be classified as semi-transparent.

European Union

Building on the objectives and requirements of the eEurope Action Plan 2002, the European Council of Barcelona asked the Commission to develop a further action plan that would improve the security of ICT infrastructures and push forward services such as e-government, e-learning, e-business and e-health. With a view to ensuring a secure information structure, the EU has already introduced a wide-ranging strategy that is based on eEurope 2002, notifications regarding the security of IT networks, computer criminality and present and future directives on the protection of the personal sphere in the area of electronic communication.

NATO

The protection of critical infrastructures comes under Information Operations (IO) within NATO and since 1997 it has been the responsibility of a working party whose members are military staff. With a view to the security of the ICT infrastructures of NATO, the NATO Consultation, Command and Control Agency (NC3A) has published important studies on its work in the field of security. These studies are concerned with encryption technologies and PKI concepts, firewalls and the flagging of network penetration.

OECD

The Guidelines for the Security of Information Systems published in 1992 were the first guidelines to be explicitly concerned with the protection of critical infrastructures. Despite their continuing universality, these guidelines have for some time been undergoing an internal review process within the OECD aimed at incorporating modifications in line with changes that have occurred since 1992. In general, OECD activities in the area of critical infrastructure protection fall into two areas: documentation aimed at significantly influencing national debates and raising awareness of the problem within governments, the business world and the public.

France

The DCSSI is the central co-ordination point for information security in the French state. The central data collection point for IT-relevant incidents is CERTA. CERTA is located in the general secretariat for national defence and is involved in global co-operation between CERTs.

Finland

Critical infrastructure protection is incorporated into the overall concept “Total Defence” and in the All Hazards approach. Individual ministries are responsible for IT security within their respective areas of responsibility. CIP/EM are regarded as the overall responsibility of civil defence and national defence. The National Emergency Supply Agency (NESA) is responsible for organising the physical protection of national critical infrastructures. Since 2002, responsibility for communication security and computer emergency response has been centralised.

Norway

The “Computer Technology and the Vulnerability of the Society” study underlined the need for a cross-sector approach to the protection of critical infrastructures within the framework of the concept of “Total Defence” and the All Hazards approach: General civil defence and the protection of IT-based critical infrastructures are being merged. There are plans to set up a Centre for Information Assurance. At the heart of the Norwegian model lies the Directorate for Civil Defence and Emergency Planning (DCDEP).
Russia
As yet there is no real competent central co-ordination mechanism in place for the whole area of national critical infrastructures. In addition to the Russian Security Council, two other government agencies are concerned with the subject of IT security: the Federal Security Service (FSB) and the Federal Agency for Government Communications and Intelligence (FAPSI). On the side of the private sector a few initiatives have taken place, but these are not very effective.

South Africa
The State Information Technology Act of 1994 was one of the first steps in the direction of systematic critical infrastructure protection. The State Information Technology Agency is responsible for looking after the area of IT security for government agencies and ministries.

India
By way of the Ministry for Information Technology, the Indian government has launched a number of initiatives under the framework of an Information Technology Action Plan. In addition, the Information Technology Act of 1999 defines a basic code for the area of e-commerce. As part of the Information Technology Act 2000, the government drew up a definitive action plan that mandated the establishment of dedicated organisations and guidelines for the area of IT security. At the present time, the Indian measures on critical infrastructure protection are not having any discernible impact.

Malaysia
The central agency involved in the protection of critical infrastructures in Malaysia is the Malaysian Communications and Multimedia Commission which was set up under the Malaysian Communications and Multimedia Commission Act. In the private sector, the National ICT Security and Emergency Response Centre that was founded by the National IT Council offers its expertise in the areas of vulnerability analysis, intrusion detection and forensic computer technology. Generally-speaking, there is a discernible lack of co-ordination and inadequate exchange of information.

China
The Chinese approach to critical infrastructure protection should be viewed as an attempt to reconcile the internal security endeavours of the state with the necessity of economic modernisation with regard to information technology. The Chinese regime views the country’s critical infrastructure assets more in terms of being threatened from outside.

Japan
The Action Plan on Building Infrastructure to Counter Hackers and Other Cyber-Threats published in January 2000 constituted the foundation stone for the co-ordinated protection of critical infrastructures in Japan. As a central document, the Special Plan on Fighting Cyberterrorism against Critical Infrastructure defines the Japanese approach to the protection of critical infrastructures. The central co-ordinating point for critical infrastructure protection in Japan is the Cabinet Secretariat.

Singapore
As far as the public sector is concerned, the tasks and functions of national critical infrastructure protection were all passed to the Infocomm Development Authority of Singapore, which reports to the Ministry of Information, Communications and the Arts, back in 1996. The country has chosen the concept of “Total Defence”, but the All Hazards approach has not been adopted. The Infocomm Security Division is the central office for the establishment and implementation of a reliable IT security structure for the (public) national ICT infrastructures in Singapore. SingCERT is the central co-ordinating body for all IT-relevant incidents. At the organisational level, critical infrastructure protection may be described as extremely centralised.
New Zealand

The New Zealand policy document on critical infrastructure protection is the E-Government Strategy dated 8 December 2000, on the back of which the Centre for Critical Infrastructure Protection (CCIP) was set up. The protection of New Zealand’s critical infrastructures is difficult to separate from measures and initiatives in Australia. There is close co-operation between the two nations.

Germany

The Critical Infrastructure Protection (CIP) Working Party of Federal Ministries was set up in Germany around the time of the report of the American President’s Commission for Critical Infrastructure Protection (PCCIP) in 1997, under the leadership of the Federal Ministry of the Interior (BMI). Since then the protection of critical infrastructures has been gaining in importance. Various campaigns, such as Security on the Internet and the setting up of special commissions (e.g. the Study Commission of the German Bundestag) are intended to increase awareness of the protection of critical infrastructures.

The Federal Office for Information Security (BSI) has a co-ordinating function here, as well as making available suitable security technologies and solutions. A strategy comparable to the national plan does not yet exist in Germany but is currently under development. The first attempts at co-operation with the private sector and also the first independent initiatives on the part of the private sector have been seen. These include, for example, the D 21 initiative, the Partnership for Secure Internet Business and the Protection of Infrastructures Working Group (AKSIS).

The CERTs are playing an increasingly important role in the protection of critical infrastructures as a result of their preventive measures against IT security vulnerabilities and the capability of responding immediately to threats and attacks. The German system for the protection of critical infrastructures is not very transparent to outsiders. Since 11 September 2001, work in the area of protection of critical infrastructures has been stepped up noticeably. The infrastructure studies carried out by the BSI in 2002 make Germany one of the few countries that are following an analytic, process-oriented approach. Several universities are carrying out research in the area of IT security.

Further Information

BSI homepage. International collection of links:
http://www.bsi.bund.de/fachthem/kritis/links.htm


---

4 Not examined in the study, section has been added in analogous fashion.
<table>
<thead>
<tr>
<th>National approach</th>
<th>National strategy</th>
<th>Government agencies and establishments</th>
<th>Co-operation with private sector</th>
<th>Transparency</th>
<th>Significance of CI protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Australia</td>
<td>Being drawn up</td>
<td></td>
<td>Co-operation</td>
<td>Semi-transparent</td>
<td>Intermediate</td>
</tr>
<tr>
<td>Germany⁵</td>
<td>CIIP Critical Information Infrastructure Protection</td>
<td>Planned for 2003</td>
<td>BSI is playing leading role Ultimate responsibility rests with the BMI</td>
<td>Various collaborations Private sector initiatives</td>
<td>Not very transparent</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>CIIP</td>
<td>Non-existent</td>
<td>NISCC⁶ (state level) IAAC⁷ (public-private level) No ultimate responsibility</td>
<td>Private sector integrated since 2001</td>
<td>Transparent up to a point</td>
</tr>
<tr>
<td>Canada</td>
<td>All Hazards CIIP + military, civil defence, disaster control</td>
<td>OCIPEP⁸ is national strategy and co-ordination organ Ministry of defence plays prominent role</td>
<td>Little integration up to now</td>
<td>Not transparent</td>
<td>Intermediate</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>CIIP</td>
<td>Being drawn up Policy document VIR 1994</td>
<td>No central state institution for control and co-ordination</td>
<td>Private sector at the centre Co-ordination problems</td>
<td>Transparent</td>
</tr>
<tr>
<td>Sweden</td>
<td>All Hazards</td>
<td>Exposed position of ministry of defence Ultimate responsibility controlled</td>
<td>Private sector successfully integrated No co-coordinating organ</td>
<td>Transparent</td>
<td>High</td>
</tr>
<tr>
<td>Switzerland</td>
<td>All Hazards</td>
<td>Ministry of defence plays leading role No central control and co-ordination organ</td>
<td>No real integration up to now</td>
<td></td>
<td>High</td>
</tr>
<tr>
<td>USA⁹</td>
<td>CIIP</td>
<td>Secure cyberspace</td>
<td>DHS¹⁰ co-ordinates government initiatives Ultimate responsibility with the White House</td>
<td>Co-operation with private industry works Co-ordination within the private sector via ISACs¹¹</td>
<td>Transparent</td>
</tr>
</tbody>
</table>

⁵ Not examined in the study, details have been added in analogous fashion.
⁶ NISCC = National Infrastructure Security Co-ordination Centre
⁷ IAAC = Information Assurance Advisory Council
⁸ OCIPEP = Office of Critical Infrastructure Protection and Emergency Preparedness
⁹ According to information as of August 2003
¹⁰ DHS = Department of Homeland Security
¹¹ ISACs = Information Sharing and Analysis Centers
<table>
<thead>
<tr>
<th>Country</th>
<th>National approach</th>
<th>National strategy</th>
<th>Government agencies and establishments</th>
<th>Co-operation with private sector</th>
<th>Transparency</th>
<th>Significance of CI protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>Controlled centrally</td>
<td>Non-existent</td>
<td></td>
<td>None</td>
<td>Not transparent</td>
<td>Low</td>
</tr>
<tr>
<td>Finland</td>
<td>All Hazards</td>
<td>Ultimate responsibility with the relevant ministries</td>
<td></td>
<td></td>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td></td>
<td></td>
<td></td>
<td>Hardly transparent</td>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>Information Technology Action Plan, no national strategy</td>
<td>Information Technology Act 2000 sets out definitive action plan</td>
<td></td>
<td>Hardly transparent</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>Action plan but no national strategy</td>
<td>Central co-ordinating point is the Cabinet Secretariat</td>
<td></td>
<td>Hardly transparent</td>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Malaysia</td>
<td></td>
<td>Central agency is Malaysian Communications and Multimedia Commission</td>
<td>National ICT Security and Emergency Response Centre – central establishment</td>
<td>Not transparent</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>New Zealand</td>
<td>E-Government Strategy 2000 policy document, No national strategy</td>
<td>Centre for Critical Infrastructure Protection (CCIP) is co-ordinating organ</td>
<td></td>
<td>Intermediate, closely linked with Australian initiatives</td>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Norway</td>
<td>All Hazards</td>
<td>Core is DCDEP(^2)</td>
<td></td>
<td></td>
<td>Intermediate</td>
<td></td>
</tr>
<tr>
<td>Russia</td>
<td>Non-existent</td>
<td>No control or co-ordinating organ</td>
<td>Several small initiatives, ineffective</td>
<td>Not transparent</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>Singapore</td>
<td>Concept of “Total Defence” but not All Hazards</td>
<td>Non-existent</td>
<td>Central co-ordinating body = InfoCom Development Authority of Singapore, Highly centralised</td>
<td>Very little</td>
<td>Hardly transparent</td>
<td>Intermediate</td>
</tr>
<tr>
<td>South Africa</td>
<td>State Information Technology Act, but no national strategy</td>
<td>State Information Technology Agency looks after government’s initiatives</td>
<td></td>
<td>Very little</td>
<td>Hardly transparent</td>
<td>Intermediate</td>
</tr>
</tbody>
</table>

\(^2\) DCDEP = Directorate for Civil Defense and Emergency Planning