.SIAK REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
SICHERHEITSAKADEMIE

# .SIAK-Journal – Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis


Hoverd, Harry (2006):

# International co-operation on Critical Infrastructure Protection

SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 26-33.

doi: 10.7396/2006_2_C

*Um auf diesen Artikel als Quelle zu verweisen, verwenden Sie bitte folgende Angaben:*

Hoverd, Harry (2006). International co-operation on Critical Infrastructure Protection, SIAK-Journal − Zeitschrift für Polizeiwissenschaft und polizeiliche Praxis (2), 26-33, Online: http://dx.doi.org/10.7396/2006_2_C.



Online publiziert: 4/2014

Harry Hoverd

# International co-operation on Critical Infrastructure Protection

**Harry Hoverd,**
works for the Home Office in the United Kingdom and is part of the Crime Reduction and Community Safety Groups Critical Infrastructure Protection Team. He joined the civil service in 1977 and has represented the UK for a number of years on European Union, NATO and G8 committees covering emergency planning and critical infrastructure protection issues. He currently sits on the G8 Lyon/Roma High Tech Crime sub-group and the NATO ad-hoc working group on Critical Infrastructure Protection. He is also one of the UK's representatives on the EU-SEC project.
e-mail:
Harry.Hoverd@
homeoffice.gsi.gov.uk

**One of the aims of the United Kingdom during its Presidency of the European Union (EU) and the G8 in 2005 was to explore avenues for improving international co-operation across a range of issues, including my own field of Critical Infrastructure Protection (CIP). I consider international co-operation in the field of CIP to be vitally important, particularly when we consider that many businesses that make up our Critical National Infrastructures are multi-national companies, whose headquarters are often based outside of our own borders. Before I continue through I think it is important to establish exactly what CIP is as the term can mean different things to different nations. So as a starting point, I will briefly outline what we understand CIP to mean in the UK, and then offer some areas for consideration where I believe international co-operation in this area could be further developed.**

**CIP within the United Kingdom.** When we refer to CIP in the UK we are really talking about protecting our critical infrastructures from an attack, be that physical or electronic, and the steps we should take to minimise the risk of such an attack. I am aware however, that within many other nations, the definition goes wider than this and includes consequence management arrangements. In the UK arrangements fall under the more general civil contingencies banner and are the responsibility of the Cabinet Office. However, for the purposes of this article, I have considered the need for international co-operation to cover all areas of Civil Emergency Planning as I feel the issues involved apply across all areas.

As a starting point, I believe I should explain exactly what I mean when I talk about the elements of the critical infrastructure. In the UK for example, infrastructure in this sense is defined as the assets, services, processes and systems that support the economic, political and social life of the UK.

The UK's Critical National Infrastructure (CNI) is defined as all the elements of infrastructure, comprising businesses, public sector organisations, operational processes, and physical locations, which if successfully attacked, would result in:

- catastrophic economic damage or disruption to the UK,
- mass casualties, and
- symbolic damage.

The UK has identified ten sectors and thirty-nine sub-sectors that make up the CNI and includes the physical (and personnel) elements of the infrastructure, and the IT infrastructure that underpins much of it.

***Vocabulary:***

*to establish = eröffnen, (be-)gründen, errichten*
*consideration = Erwägung, Überlegung*
*assets = Vermögenswerte*
*disruption = Zerbrechen, Zerreißen, Spaltung*
*casualties = Opfer*
*underpin = unterstützen, untermauern*

**The United Kingdom's ten Critical National Infrastructure Sectors.**

| | |
|---|---|
| • Energy | • Health |
| • Government | • Emergency Services |
| • Finance | • Food & Drink |
| • Telecoms | • Public Safety |
| • Water | • Transport |

CIP within the UK can therefore be further defined as the preservation of the functionality of the defined elements of the critical infrastructure. Below is a table of UK definitions in this field which can be used as useful reference points.

**Terms and UK Definitions:**

• **Vulnerability.** The susceptibility of a community, services or infrastructure to damage or harm by a realised hazard or threat.

• **Consequence Management.** The process of managing the consequences of an emergency event, including the maintenance of procedures to assess, prevent, prepare for, respond to and recover from the emergency.

• **Critical Information Infrastructure (CII).** - The critical information infrastructure elements of one or more CNI sectors,

- The IT and communications systems that provide critical services.

• **Critical Information Infrastructure Protection (CIIP).** The protection of the CII, usually by means of advice to owners of CII elements. This advice may sometimes need to be applied well beyond the boundaries of core CNI systems due to the extensive interconnectivity of most IT systems.

• **Critical Infrastructure Protection (CIP).** The preservation of the functionality of the defined elements of the critical infrastructure.

• **Impact.** The scale of the consequences of a hazard or threat expressed in terms of a reduction in human welfare, damage to the environment, and loss of security. Impact can be measured both qualitatively (low, medium, high) and quantitatively (money, time, performance).

• **Incident.** An occurrence, either human caused or by natural phenomena, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring an emergency response.

• **Infrastructure.** The assets, services, processes and systems that support the economic, political and social life of the UK.

• **Protective Security.** This is concerned with providing a set of balanced complementary measures that reduce the vulnerabilities of an identified target from attack. These measures normally need to include:
• Physical security,
• Personnel security,
• IT security.

***Vocabulary:***

*preservation = Erhaltung*
*susceptibility = Anfälligkeit*
*hazard = Gefahr*
*to assess = einschätzen*
*to spill = ver-, ausschütten*
*complementary = ergänzend*

Critical Infrastructure Protection within the UK can therefore be further defined as the preservation of the functionality of the defined elements of the critical infrastructure.

An Incident is an occurrence, either human caused or by natural phenomena, that requires an emergency response to protect life or property.

Infrastructure: The assets, services, processes and systems that support the economic, political and social life of the UK.

• **Risk.** Risk measures the significance of a potential event in terms of likelihood (probability of occurrence) and impact (magnitude of effect).

• **Risk Assessment.** A structured and auditable process of identifying potentially significant events, assessing their likelihood and impacts, and then combining these to provide an overall assessment of risk, as a basis for further decisions and action.

• **Threat.** The intent and capacity to cause loss of life or create adverse consequences to human welfare (including property and the supply of essential services and commodities), the environment or security.

The UK has developed well established international contacts and regularly shares CIP information across our borders both bi-laterally and multi-laterally.

**Existing international co-operation.** The UK has developed well established international contacts and regularly shares CIP information across our borders both bi-laterally and multi-laterally. International co-operation has been particularly successful in the field of Critical Infrastructure Information Protection (CIIP) and two examples, of this are considered below.

In 2003 the G8 Justice and Home Affairs Ministers adopted a set of eleven principles for protecting critical information infrastructures.

**The G8 "Critical Infrastructure Information Protection Principles".** In 2003 the G8 Justice and Home Affairs Ministers adopted a set of eleven principles for protecting critical information infrastructures. In doing so they announced that information infrastructures form an essential part of critical infrastructures which need to be protected from damage and attack. They added that effective protection requires communication, co-ordination and co-operation nationally and internationally among all stakeholders including academia, the private sector and government entities including infrastructure protection and law enforcement agencies. These principles, which are non-binding, cover a range of recommendations including "Countries should engage international co-operation, when appropriate, to secure critical information infrastructures, including by developing and co-ordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents, and co-ordinating investigations of attacks on such infrastructures in accordance with domestic laws."

One of the aims of the G8 group of Nations is to share these principles with as many other nations as possible and as such, the UK is keen to encourage as many other nations as possible to consider adopting them. The full text of the Ministerial announcement and the eleven principles follows: Information infrastructures form an essential part of critical infrastructures. In order effectively to protect critical infrastructures, therefore, countries must protect critical information infrastructures from damage and secure them against attack. Effective critical infrastructure protection includes identifying threats to and reducing the vulnerability of such infrastructures to damage or attack, minimising damage and recovery time in the event that damage or attack occurs, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement. Effective protection also requires communication, co-ordination, and co-operation nationally and internationally among all stakeholders – industry, academia, the private sector, and government entities, including infrastructure protection and law enforcement agencies. Such efforts should be undertaken with due regard for the security of information and applicable law concerning mutual

***Vocabulary:***

*auditable = prüfbar*
*adverse = widrig, gegnerisch, feindlich*
*commodities = Waren, Rohstoffe*
*vulnerabilites = Verwundbarkeit*

legal assistance and privacy protection. To further these goals, we adopt the following Principles and encourage countries to consider them in developing a strategy for reducing risks to critical information infrastructures.

1. Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

2. Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures, and the role each must play in protecting them.

3. Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures.

4. Countries should promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.

5. Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

6. Countries should ensure that data availability policies take into account the need to protect critical information infrastructures.

7. Countries should facilitate tracing attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other countries.

8. Countries should conduct training and exercises to enhance their response capabilities and to test continuity plans in the event of an information infrastructure attack and should encourage stakeholders to engage in similar activities.

9. Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures and to co-ordinate such investigations with other countries as appropriate.

10. Countries should engage international co-operation, when appropriate, to secure critical information infrastructures, including by developing and co-ordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats, and incidents, and co-ordinating investigations of attacks on such infrastructures in accordance with domestic laws.

11. Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

Countries should have emergency warning networks regarding cyber vulnerabilities, threats, and incidents.

Countries should promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate, and respond to damage to or attacks on such infrastructures.

**The G8 "International Critical Infrastructure Information Protection Directory".** Another very useful piece of work in this area to come out of the G8 is the International CIIP Directory, which contains government and police contact details for eighteen countries when dealing with international CIIP investigation enquiries. The Directory, which is currently in its eighth edition, is maintained by the National Infrastructure Security Co-ordination Centre (NISCC) in the UK, and is constantly expanding as international government departments add their details for inclusion. This is another area that the UK seeks to encourage other nations who do not currently contribute to the directory, to consider doing so. The initial contact point for the Directory is ciip-directory@niscc.gov.uk.

Another very useful piece of work in this area to come out of the G8 is the International Critical Information Infrastructure Protection Directory, which contains government and police contact details for eighteen countries when dealing with international Critical Information Infrastructure Protection investigation enquiries.

***Vocabulary:***

*interdependencies = gegenseitige Abhängigkeit*
*availability = Vorhandensein, Verfügbarkeit*
*prosecute = gerichtlich/strafrechtlich verfolgen*
*inclusion = Einbeziehung*

**Critical infrastructure protection work in international organisations.** A number of international organisations are involved in work concerning CIP. Some of this work is duplicated across the various bodies involved and currently there is little or no co-operation between these bodies. For the purposes of this paper I have considered three of the main organisations that the UK is a member state. These are NATO, the European Union and the G8.

A number of international organisations are involved in work concerning Critical Infrastructure Protection. Some of this work is duplicated across the various bodies involved and currently there is little or no co-operation between these bodies.

**NATO.** CIP work is currently being undertaken by NATO via an ad-hoc working group. This group, which is co-chaired by Canada and the UK, was set up in 2000 and is currently considering a number of CIP related issues for sharing information between the Alliance members and their partnership for peace members. In September 2005 Moldova hosted a CIP seminar on behalf of NATO and a number of recommendations for the future work in this area were proposed for the working group to consider taking forward. One of these recommendations was to consider ways of developing links with other international organisations in order to avoid duplication and identify areas where they can work together or share ideas and initiatives.

The European Union has recently issued a paper on the "European Programme for Critical Infrastructure Protection".

**The European Union.** The European Union has recently issued a paper on the "European Programme for Critical Infrastructure Protection". This is a far reaching document which makes a number of recommendations for further work in this area and will clearly need to be considered very carefully by the member states.

**The G8.** The G8 nations have been discussing CIIP work for a number of years now as part of the work of the Lyon/Roma Groups High Tech Crime sub-group. I have already mentioned two of the initiatives to come out of this group in this area so will not say anymore here.

Considering the cross membership of these three organisations I consider it to be desirable that there should be some form of co-operation between them, and other such like bodies, to avoid duplication of effort and to enable and encourage the sharing of ideas and initiatives. The alternative is that we will have such organisations working in isolation and issues that may well have already been covered by another organisation or organisations. Apart from the waste of resources involved, member states often find themselves being asked to supply similar information to a number of different international organisations which can be time consuming and frustrating.

**The United Kingdom's Protective Security Principles.** The main priorities for Protective Security of the UK critical infrastructure are to prevent damage to economic targets, and to prevent mass casualties. The principles that are applied in order to achieve this are:

- To safeguard the public and minimise disruption to normal daily life;
- To ensure that those people and organi-

***Vocabulary:***

*to concern = von etw. handeln, behandeln*
*recommendation = Empfehlung*
*to propose = vorschlagen, beabsichtigen*
*to mention = erwähnen*
*desirable = erstrebenswert, begehrt*

sations in both government and in Private Sector who need to protect from, and respond to, attack can do so effectively;
• To enable all businesses and organisations to understand the risks they face, and be in a position to apply a proportionate level of security measures to protect themselves, their employees and their assets;
• To ensure that there is a robust approach to prioritisation of targets, underpinned by effective Risk Management, and in particular driven by the assessment of impact.

The specific objectives of protective security measures are:
• stopping attacks,
• deterring attacks through target hardening and
• reducing the impact of an attack.

Some Principles That Could Be Applied to International Organisations for Critical National Infrastructure Protection:

Some examples of the types of principles that could be applied across international organisations are as follows:
• Responsibility for the protection of infrastructure lies primarily with the owner/operator of that infrastructure.
• Information will only be shared on a strictly need-to-know basis, and will only be shared if not counter to the interests of National Security.
• Each Member State is responsible for testing their own infrastructure's Consequence Management plans.
• Each Member State is willing to share its expertise and good practises to help other Member States. UK expertise which could be offered to international bodies include:
  - Risk Assessment methodology, i.e. Risk Assessment of identified targets, by assessment of Impact, Vulnerability & Threat.
  - UK definitions of these terms, and criteria used.
  - Risk work is also being undertaken in the Civil Protection Working Party and the link between CIP and civil protection should not be overlooked.
• Member States will co-operate sharing appropriate threat and intelligence information and, in the event of an incident, ensuring co-ordination of information to MS.
• Existing effective bilateral agreements on shared trans-border infrastructure will not be compromised.
• Co-operative partnerships with the private sector owners/operators is the most effective approach to improving CIP.

Some Principles That Could Be Applied at Member State Level for Critical National Infrastructure Protection:
• Responsibility for managing the National critical infrastructure, and their interdependencies, remains with the Member State
• Responsibility for the protection of infrastructure lies primarily with the owner/operator of that infrastructure.

We would emphasise that this concern over unnecessary sharing of sensitive data is not an issue of trust. It is more a reflection of our underlying philosophy that security-related data is only shared on a “Need to Know” basis.

Responsibility for the protection of infrastructure lies primarily with the owner/operator of that infrastructure.

Information will only be shared on a strictly need-to-know basis, and will only be shared if not counter to the interests of National Security.

We would emphasize that this concern over unnecessary sharing of sensitive data is not an issue of trust. It is more a reflection of our underlying philosophy that security-related data is only shared on a “Need to Know” basis.

***Vocabulary:***

*to deter = abschrecken, abhalten*
*responsibility = Verantwortung, Zuständigkeit*
*appropriate = angemessen, angebracht*
*to compromise = schaden, dem Ansehen schaden, kompromittieren*
*to emphasise = betonen, hervorheben*

**Some barriers to international co-operation.**

**National Security.** There are of course certain areas where international co-operation will not always be possible due to issues concerning national security. This is not to say that nations will not share information with trusted partners on security issues, but it must always be for individual nations to decide just what information regarding security issues they are prepared, or allowed by national law, to share.

Language can often be a barrier to international co-operation, particularly when it comes to requests for sharing of certain information.

**Language.** Language can often be a barrier to international co-operation, particularly when it comes to requests for sharing of certain information. Simply not understanding exactly what is required, when by and in what form. Within NATO, French and English are the accepted working languages, but for international co-operation to be truly effective between the member states in the CIP arena, it needs to be able to work at all levels, including government, police and other investigative agencies.

By working together nations should be able to identify and agree on future aspects of work in this important and developing field.

**Not Knowing Who to Contact.** Fairly simple, but a fairly common barrier to international co-operation is an official in one country not knowing who to speak to in other countries. The establishment of an International CIP Contact Directory, based on the G8 CIIP International Contact Directory discussed earlier, is one possible way to help overcome this. Another of the recommendations to come out of the NATO CIP seminar held in Moldova was to task the ad-hoc working group on CIP to investigate this further.

**Conclusions.** The UK is firmly of the opinion that there is a strong case for international co-operation in the field of Critical Infrastructure Protection between national governments and international bodies such as NATO, the European Union and the G8, and that such international co-operation would have a number of benefits for all concerned. However, we also strongly believe that there are areas, particularly those concerning national security, that are best left to national governments to take forward. By working together nations should be able to identify and agree on future aspects of work in this important and developing field.

***Vocabulary:***

*investigative agency = Untersuchungsbehörde, ermittelnde Behörde*
*establishment = Unternehmen, Organisation*
*to investigate = untersuchen, nachgehen*
*to develop = sich entwickeln, entfalten*

# Zusammenfassung

***Wenn wir vom Schutz kritischer Infrastrukturen (Critical Infrastructure Protection – CIP) im Vereinten Königreich sprechen, so reden wir tatsächlich über den Schutz unserer kritischen Infrastrukturen vor Angriffen, seien diese physischer oder elektronischer Natur, und über die Maßnahmen, die getroffen werden müssen, um das Risiko solcher Angriffe zu minimieren. Im Vereinten Königreich ist das Civil Contingencies Secretariat zuständig für diese Vorkehrungen, die im Zuständigkeitsbereich des Cabinet Office liegen.***

***Für die Zwecke dieses Artikels wurde jedoch die Notwendigkeit, dass die internationale Kooperation alle Bereiche der Staatlichen Notfallplanung abdeckt, betrachtet, weil ich der Meinung bin, dass die auftretenden Probleme auch diese Bereiche betreffen. Die Kritischen Nationalen Infrastrukturen (Critical National Infrastructure – CNI) des Vereinten Königreichs sind definiert als all die Elemente der Infrastruktur, einschließlich Geschäftswelt, Organisationen im öffentlichen Dienst, operative Prozesse und Örtlichkeiten, deren Beschädigung oder Zerstörung im Falle eines erfolgreichen Angriffs zu katastrophalen ökonomischen Schäden, der Zerrüttung des Vereinten Königreichs, Massenverlusten und/oder symbolhaftem Schaden führt. Daher kann der Schutz der kritischen Infrastrukturen innerhalb des Vereinten Königreichs genauer als Erhaltung der Funktionalität der oben definierten Elemente der kritischen Infrastrukturen definiert werden. Das Vereinte Königreich hat wohl etablierte internationale Kontakte geknüpft und tauscht regelmäßig – sowohl bi- als auch multilateral – Informationen, den Schutz kritischer Infrastrukturen betreffend, aus.***

***Die internationale Kooperation war im Bereich des Schutzes der kritischen Informations- und Telekommunikationsinfrastrukturen (Critical Information Infrastructure Protection – CIIP) besonders erfolgreich, belegbar durch die beiden Beispiele G8 "Schutz internationaler kritischer Informations- und Telekommunikationsinfrastrukturprinzipien" (Critical Infrastructure Information Protection Principles) und G8 "Schutz internationaler kritischer Informations- und Telekommunikationsinfrastrukturrichtlinien" (International Critical Infrastructure Information Protection Directory).***

***Eine Reihe von internationalen Organisationen ist an Tätigkeiten, die den Schutz der kritischen Infrastrukturen betreffen, beteiligt. Teile dieser Tätigkeiten werden von den unterschiedlichen Organisationen doppelt ausgeführt. Derzeit gibt es wenig bis gar keine Kooperation zwischen den besagten Organisationen. Zum Zwecke dieser Abhandlung habe ich drei Hauptorganisationen in Betracht gezogen, deren Mitglied das Vereinte Königreich ist. Das sind die NATO, die Europäische Union und die G8.***

***Das Vereinte Königreich ist der festen Überzeugung, dass es triftige Gründe für eine internationale Kooperation auf dem Gebiet des Schutzes der kritischen Infrastrukturen zwischen nationalen Regierungen und internationalen Organisationen, wie der NATO, der Europäischen Union und den G8 gibt, und dass diese internationale Kooperation eine Reihe an Vorteilen für alle Beteiligten mit sich bringen würde.***

Im Vereinten Königreich ist das Civil Contingencies Secretariat zuständig für diese Vorkehrungen, die im Zuständigkeitsbereich des Cabinet Office liegen.

Das Vereinte Königreich hat wohl etablierte internationale Kontakte geknüpft und tauscht regelmäßig – sowohl bi- als auch multilateral – Informationen, den Schutz kritischer Infrastrukturen betreffend, aus.

Eine Reihe von internationalen Organisationen ist an Tätigkeiten, die den Schutz der kritischen Infrastrukturen betreffen, beteiligt. Teile dieser Tätigkeiten werden von den unterschiedlichen Organisationen doppelt ausgeführt.