

RAND

Managing New Issues

*Cyber Security in an Era
of Technological Change*

*Report on a conference held at
The Hague, The Netherlands
9 April, 2001*

*Marten van Heuven, Maarten Botterman,
Stephan de Spiegeleire*

RAND Europe

ISBN: 0-8330-3334-4

RAND is a nonprofit institution that helps improve policy and decisionmaking through research and analysis. RAND[®] is a registered trademark. RAND's publications do not necessarily reflect the opinions or policies of its research sponsors.

© Copyright 2003 RAND

All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from RAND.

Published 2003 by RAND

1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

1200 South Hayes Street, Arlington, VA 22202-5050

201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516

RAND URL: <http://www.rand.org/>

To order RAND documents or to obtain additional information, contact Distribution Services:

Telephone: (310) 451-7002; Fax: (310) 451-6915; Email: order@rand.org

Contents

<u>Preface</u>	7
<u>Introduction</u>	9
<u>Summary</u>	11
<u>Nature of the Report</u>	11
<u>The Threat</u>	11
<u>Tackling the Problem</u>	12
<u>Roles for Government and Industry</u>	13
<u>Key Issues</u>	14
<u>Next Steps for Europe</u>	14
<u>Europe-US Cooperation</u>	14
<u>Key Findings</u>	15
<u>Framing the Question: What Are the Threats and What Is the Matrix of Possible Responses?</u>	17
<u>How Should the Public and Private Sectors Work Together?</u>	21
<u>Next Steps for Europe</u>	25
<u>How Should Europe and the United States Cooperate?</u>	27
<u>Challenges/Suggestions</u>	29
<u>Understanding the Problem</u>	29
<u>Technical Requirements</u>	29
<u>The Trust Issue</u>	29
<u>Additional Players</u>	30
<u>Regulation</u>	30
<u>Legislation</u>	30
<u>Law Enforcement</u>	31
<u>Subsidiarity</u>	31
<u>Strengthening the Cyber Security Community</u>	31
<u>Annex 1 – Conference Agenda</u>	34
<u>Annex 2 – List of Participants</u>	36

Preface

This report is based on the Conference on Cyber Security co-organized by the US Embassy in The Hague and RAND Europe on April 9, 2001 in The Hague. It is the product of the efforts of many organizations and individuals, both organizers and participants.

The conference was born of a conversation between Ambassador Cynthia Schneider and David Gompert, President of RAND Europe and both continued to play a leadership role in converting the vision of a conference into reality.

The American Embassy in The Hague, under the direction of Ambassador Cynthia Schneider, played a seminal role in the preparation for and the conduct of the conference. Public Affairs Counsellor Angier Peavy effectively organized the preparatory meeting at the Embassy and ran the conference with verve, ably assisted by Embassy staff. Counsellor for Economic Affairs Mark Tokola was indefatigable in putting together the roster of speakers, and in organizing the preparations as well as the follow-up.

Royal Dutch Shell was a strong supporter of the conference from the beginning. Its enthusiastic sponsorship was personified by Pieter van Dijken, whose energetic and ever constructive role smoothed out key difficulties.

Ultimately, it was the diverse and informed group of speakers, the panel chairmen, and the participants in the discussion who gave life to the conference and who gave shape to the issues and questions that this report seeks to capture.

RAND Europe is an independent not-for-profit policy research organization that serves the public interest by improving policymaking and informing public debate. This report has been peer-reviewed in accordance with RAND's quality assurance standards (see <http://www.rand.org/about/standards/>) and therefore may be represented as a RAND Europe product.

For more information please see <http://www.randeurope.org>.

Introduction

In recent years, with the growth of the Internet, attacks on computer networks have caused economic losses and created risks for national infrastructure security. Losses are estimated in the billions of dollars. Attacks have been directed against both commercial and government infrastructure systems. In addition, criminals around the world are increasingly using computers to commit traditional crimes, such as financial fraud, distribution of child pornography, and copyright piracy.

The March 7, 2001 public hearing held in Brussels by the European Commission on cyber crime demonstrated that there is a need for increased consensus between the private sector, governments, and law enforcement officials to find the best means to counter hackers, computer virus spreaders, denial of service attacks, and use of the internet for illicit purposes. Not only IT companies, but also all companies who do business over the Internet have a vital interest in promoting the best form and degree of security and regulation.

The April 9 conference addressed three themes regarding the role of the public and the private sector in dealing with cyber security and cyber crime:

- What are the threats and what is the matrix of possible responses?
- How should Europe and the United States cooperate?
- How should the public and the private sector work together?

The conference that gave rise to this report was the brainchild of the American Ambassador in The Hague, Dr. Cynthia Schneider and of David Gompert, President of RAND Europe. Together they laid the foundation for cooperation between the American Embassy in The Hague and RAND Europe in Leiden, The Netherlands. They envisioned the conference as a first step toward what is likely to be a global dialogue. The effort was sponsored by Royal Dutch Shell, which gave strong support throughout.

From the beginning, there was agreement to distil the essence of the conference in a report. RAND Europe undertook the task of preparing and distributing the report. The purposes of this report are:

- To capture the issues raised at the conference
- To provide information and analysis to the select but growing number of industry representatives and government officials directly involved in managing cyber security issues, and
- To inform the wider interested public

Thus, this report, though broad, is limited. It reflects what the speakers and participants said at the conference. Thus, there will be some repetition, as a number of themes resurfaced in successive sessions. The attentive reader will also notice some apparent contradictions: the assertion that there are no fundamental policy differences between the

United States and Europe stands alongside the observation that the approach towards cyber security originates from different angles. On issues involving societal values the two continents exhibit marked differences.

While providing abbreviated descriptive information that was introduced by the speakers, the report focuses on analytical issues. The sections containing Key Findings and Challenges/Suggestions are attempts by the authors of the report to describe principal issues. The report also includes their insights gained in preparing for the conference. However, the report does not purport to cover the full range of issues relating to cyber security and the problems of how to deal with them. Nor does it seek to cover the existing literature on the subject, though some will be cited.

It is the hope of the authors and sponsors that this report will be a useful contribution towards forms of understanding and cooperation that lead to a degree of security in the cyber information field that the public wants and expects.

In preparing the conference, the organizers faced the challenge of how to structure the discussion. Their approach is reflected in the headings for the different parts of the discussion:

- Framing the Question: What Are the Threats and what is the Matrix of Possible Responses?
- How Should the Public and the Private Sector Work Together?
- Next Steps for Europe
- How Should Europe and the United States Cooperate?

To the extent that the discussion at the conference permitted, the report will also follow this outline. However, the authors deemed it useful to add two headings to enhance the usefulness of the report. One heading is entitled Key Findings. It provides a summary of the principal issues. The other heading is Challenges/Suggestions. It attempts to convert the discussion at the conference into actionable future policies and programs. Finally, there is a Summary section for the busy reader.

Though the report contains some direct quotes, it will not cite individuals. An exception has been made, however, for the remarks of the representatives of the sponsoring organizations at the outset of the proceedings, and occasionally later on.

Summary

On April 9, 2001, the American Embassy at The Hague and RAND Europe organized a day-long conference to examine the challenges posed by the panoply of possible threats to cyber security and the question of how to cope with these threats. Royal Dutch Shell Company generously helped sponsor the conference.

The issue before the conference was how government and industry should organize to deal with cyber security threats. The particular questions before the conference were (1) How the United States and Europe are approaching the challenge of public-private cooperation in dealing with this danger, (2) How the public and the private sector should work together, and (3) How Europe and the United States should cooperate.

The conference was timely, given the global incidence of hacker and other interference with cyber systems and the potential of major damage. The venue made sense, given the intention of The Netherlands to become an information hub.

An array of speakers who are leaders in their fields addressed the conference. They are listed in the program (Attachment A). The list of attendees is at Attachment B.

Nature of the Report

The conference proceedings were recorded. The full, unedited text is available on-line at <http://www.randeurope.org>. This report will focus on the issues that emerged from the discussion, rather than seek to replicate it in abbreviated form. This report will also seek to bring out the differences in conceptual views and policy approaches that emerged during the day's discussion, even though participants seemed more comfortable adding their views to the debate rather than pursuing disagreements.

It is the hope of the sponsors that this report will contribute to a better understanding and a wider public debate.

The Threat

There is no such thing as perfect security. There is truth to the remark attributed to former Secretary of State Dean Rusk that at any time of the day or night, two thirds of the people in the world are awake, and some of them are up to no good. There are people who, working alone, with others, or through governments, are out to do deliberate harm. There are no "solutions" to the issues surrounding cyber security; the best we can do is to manage them. The policy aim should be to keep the "noise level" down to publicly acceptable levels.

Moreover, threats often come from within – for example from dissatisfied employees or inattention to internal security procedures. Building walls is of no use in meeting threats originating within the fortress. Serious cyber attacks from the outside, as opposed to

nuisance attacks and simple vandalism, are most likely to come from organizations with major resources.

Right now, the threat is regarded as neither immediate nor overwhelming. But, even as opinions vary as to whether future threats will be less or worse, many experts expect a high impact event somewhere in the (near) future. Comparison has been made to the oil disaster with the Exxon Valdez: a disaster like this is likely to happen. This will bring the risk high onto the agenda of decision makers and politicians.

Under these circumstances, it is important to have certifiably secure software, to distinguish individuals and organisations that can be trusted to behave, and to make efforts at self-protection. Industry should insist with software providers on a transparent market (open, non proprietary software), encourage insurers to determine risk standards, employ better auditing methods for risk assessment, and aim for better certificates of authentication (either by trusted third parties, government or self certification). Government in its turn needs to see to it that the public interest is taken into account, and needs to play its role in prevention and prosecution of crime.

The time to do these things is now. At any time, cyber space is affected by a large number of relatively low-nuisance problems that impact on confidentiality, integrity, and the availability of information. Even these can be costly - an hour's interruption of a manufacturing process can run into millions of dollars. But low-probability/high-impact events are also bound to occur. It makes sense to get ready now to meet them. One key way of doing so is to build redundancy and avoid single points of failure.

Tackling the Problem

We are still struggling to understand the nature of the problem of cyber security. A fundamental element of the problem is the unprecedented gap between the vertiginous pace of technological change and the inevitably glacial pace of policy and law making. The intractability of cyber security issues is due in part to the distributed nature of the digital infrastructure. This suggests the need for distributed approaches instead of the more traditional single, concentrated approach.

There are two ways of viewing the process: Top-down and bottom-up. The first is represented mostly on the continent of Europe. It reflects the Napoleonic legal tradition of legislating order. The second is reflected more in American and British practice. It reflects the common law approach of bringing order into human affairs case by case.

Despite this distinction, practice reflects a mix of these approaches on each side of the Atlantic. In the United States, Presidential Decision Directive (PDD) 63, while issued by government and outlining Executive responsibilities, in essence provides the tool not just for government coordination but also for government-industry cooperation. Both Council of Europe and European Union Commission approaches, meanwhile, involve interface with the private sector.

The first approach is reflected in the Convention on Cyber Crime of the Council of Europe. The purpose of this piece of international legislation is to improve international cooperation through agreed procedures for the prosecution of cyber crime. The Convention criminalizes certain forms of behaviour, establishes investigative procedures, and provides a framework for mutual legal assistance. This approach is also reflected in the effort on the part of the EU Commission to begin shaping what is intended to be a uniform EU legal system governing cyber crime.

Another approach is to tackle the problem of cyber threats at the industry level, through Information Sharing and Analysis Centres (ISACs), and at intergovernmental level by using existing machinery, such as the G-8, the Council of Europe, the EU-US Transatlantic Dialogue, as well as bilateral and private venues. Since the same people show up at all these meetings, there is no need for extra venues. The objective is to maximize the exchange of ideas and to improve mutual understanding of different ways of handling cyber threats. Flexible use of existing organizations to share information and to enhance understanding about cyber security issues can lead to better practices.

As a general rule, market-driven approaches have much to recommend themselves. There are practical steps that can be taken to mitigate the problems associated with cyber security:

- More secure software and dependable technology
- Standards that are kept up to date
- Involvement of new players, such as insurance and security companies, stock markets, and issuers of authentication certificates underwriting to which standards are kept up.

Roles for Government and Industry

The roles of industry and government are complementary. Industry has to be on top of Internet Protocol technology. Government looks to industry to protect industry information and to exercise due diligence.

Sharing information, assessments, and indications of warning are also industry responsibilities, though government can assist with these activities.

Government for its part can stimulate industry by disseminating information, stimulating R&D, facilitating interface between software makers and users, and promoting alert systems.

Moreover, government can set rules establishing criminal conduct, prosecute cyber crimes, and provide rules with respect to liability to facilitate the private settlement of disputes. Government can also provide crisis response teams to help cope with cyber attacks and the disruption of services.

Industry is hesitant to share sensitive information too widely - out of a concern for losing competitive advantage - it has been more forthcoming to share information with government in some European countries. For its part, government can act only on the

basis of information that it receives; prosecution of cyber crime will not be effective unless the victim is willing to report it.

Advanced forms of government roles in cyber protection that work in one country, such as in Sweden, may not be practical or acceptable elsewhere. The British Internet Crime Forum has made good progress in coordinating government/industry responses to cyber crime. Its mode of operation, however, requires more transparency to gain public acceptance. The ISACs in the US are beginning to work better, but they are far from functioning as well as they might.

Key Issues

We need a better understanding of the issues relating to cyber security. Technology is changing fast, but its effects on cyber security are still poorly understood. Thus, information sharing is crucial, especially in a setting where technology is moving from walled compounds to open sharing. Moreover, effective information sharing is based on trust. Law enforcement, for instance, cannot be effective if industry is hiding its losses. Government needs for data retention must be balanced against public needs for privacy.

Cyber security is a distributed problem, partly because of the distributed nature of the underlying infrastructure, and partly because industries, government and individuals all come at it with different perspectives. Under these circumstances, regulation is best attempted from the bottom up. Moreover, legislation, especially in the area of criminal law, should be sharply focused.

Next Steps for Europe

The European Commission has started to address the issue of cyber crime. This was a natural step, following earlier Commission Directives on electronic commerce, data protection, and electronic signatures. However, EU member countries already have national legislation on the books, and there is little harmony. Moreover, there is persistent uncertainty about the nature of the problem. So the EU will move with caution. Current patterns of EU-US cooperation are viewed as functional and satisfactory.

Europe-US Cooperation

There is a solid consultative network in place, fostered and stimulated by the European Commission and other players. It is effective, especially in law enforcement. There is no need for additional venues. However, there are differences in approach among industries and on the part of governments. Also, we are seeing a patchwork of consultative patterns. These factors militate against attempts at global regulation and legislation. Nonetheless, the Council of Europe's efforts to agree on terminology, and to define what actions are criminal, are useful. Other initiatives that can close the gap in understanding and stimulate cross sector and cross border cooperation are taking place.

Key Findings

The threat to information infrastructures is real. Threats run the gamut of possibilities, from faulty software to groups or hostile states intending to inflict damage. There is no agreement on whether the threat is waning. Overcoming the childhood diseases of current technology may abate the threat. On the other hand, more complicated technology may create greater vulnerabilities. Awareness of the threat varies. It gets ample and concerned attention from cyber security experts in industry and government. However, CEOs and top government officials, perhaps complacent after the Y2K experience, do not count cyber security among their top five concerns.

Cyber technology is changing rapidly and relentlessly, away from walled domains to open information sharing systems. This increases risks to data protection for industry and privacy for individuals. The road ahead is strewn with paradoxes:

- Open sharing of information contrasts with data and privacy protection.
- The problem is global; the response is sectoral or national.
- Technological change is rapid; regulation is slow.
- Law enforcement wants data retention and access; industry and the public worry about costs and privacy.
- Government and industry must share trust to cooperate effectively; nonetheless a healthy distrust of government remains a key element in this relationship.
- Different societal values produce different judgments on where to draw the lines; Americans prefer a limited role for government while Europeans tend to be more comfortable when government takes the lead.

Governance is key to effective action.

- Information infrastructure assets are mostly privately owned. This puts a premium on industry wide cooperation. Such cooperation, however, has grown piecemeal, at different speeds in different sectors. Moreover, models of cooperation that work in one place do not necessarily work in another. Nevertheless, there has been some success in creating “best practices” models.
- Government plays an indispensable role in the areas of legislation and law enforcement. Experience suggests, however, that legislation, if drawn too broadly, may have unintended consequences. Moreover, a lead role by government may create distrust.
- Government has in some cases adopted promising approaches to education and the training of experts. Government has also promoted the establishment of industry standards, as in the field of authentication of information protocols.

As awareness of vulnerability has increased, so has the number of information security experts, in industry as in government. While this group is heterogeneous - some are experts in technology, others in procedure, still others in regulation, yet others in law enforcement - they increasingly constitute a fraternity/sorority. They communicate with, and assist each other. Their network is growing in density. Private efforts, such as Esther Dyson’s Edventure Holdings, and government efforts, such as in the EU Commission, provide ever stronger glue drawing these groups of experts together.

The issue is how to manage the problem.

- Software hides many imperfections; there is a need for transparency in the software market.
- The greater danger is from within, i.e. from possibly careless or malevolent insiders.
- It pays to follow security procedures meticulously.
- It also pays to share information, even if anonymously, about threats, prevention, deterrence, failure and loss.
- Regulation should have the benefit of full consultation with the affected private sector. This is best done at the lowest level, i.e. bottom-up. Legislation should be focused rather than broad, particularly in the area of law enforcement.
- “Best practices” should be devised, discussed, applied, shared and modified in the light of experience.
- Industry standards, such as in the field of authentication, are useful.
- Other players should be brought into the process:
 - Software vendors, subject to industry pressures for the best possible product.
 - Security companies, a growing sector with presently mixed incentives.
 - Insurance companies with an incentive to improve prevention.
 - Auditing firms, which could provide independent and public assessment.
 - Stock markets and their regulators, which could add transparency to vulnerabilities.
 - Issuers of certificates of authorization, who could enhance trust.

Despite gently prodding questions by Ambassador Schneider as to why these difficult issues did not trigger more controversy, the discussion revealed broad if tentative consensus. In fact, participants tended to eschew leaps into the future, opting for a careful and incremental approach to what was admittedly a set of qualitatively new issues. It remains to be seen whether, with the pace of technological change and the rapid increase of use of the Internet, the consensus approach will be durable. This prompts the question whether, had the questions before the conference been posed more sharply, the discussion might have brought out greater differences of opinion. Any follow-up meeting should attempt to pose questions in such a way as to bring out differences of opinion and assessment that remain under the surface today.

The importance of industry standards for authentication is obvious, as is the obligation of due diligence: “It is everybody’s duty and privilege to ask: ‘who am I dealing with? Where do you come from? Who certified you? How can I trust you?’”

Equally obvious is the need for training and education. There is a role here for industry, government and academia.

Finally, harmonization is like the Holy Grail: The objective is always worth pursuing, but it is never quite within reach.

Framing the Question: What Are the Threats and What Is the Matrix of Possible Responses?

Cyber security is subject to a wide range of potential threats: Malfunctioning “crappy” software, insiders with a grudge, hackers, groups with commercial and/or political objectives, or hostile states. Harm can be accidental or intentional. Threats exist at different levels - within organizations, across organizations within one country, or organizations in many countries. The prevailing sense seems to be that the threat is neither immediate nor overwhelming. Incidences of damage due to poor software or viruses, while frequent, have not been catastrophic. The current exposure of industry to incidents causing loss is regarded as high probability/low impact.

The current threat from political action groups and hostile organizations or regimes is thought to be limited by a number of factors. First, the effects are hard to predict. This may make cyber attacks less attractive to potential actors. The interconnections of the networks and the underlying infrastructures continue to be only partly understood. Hence the consequences of cyber attacks may greatly exceed, or fall well short of, what is intended. Also, there is the possibility of third party players with different aims jumping on the band wagon, thus diluting the desired effects of the initiators: an action in cyber space may attract unexpected participants. Second, the fact that damage assessment is difficult reduces the blackmail potential of cyber attacks. Third, cyber attacks do not have the dramatic impact of conventional terrorist acts, like bombs (or, as dramatically shown recently, the use of civilian airliners against ground targets). Fourth, most criminal groups do not have the resources required for effective action. Well-targeted cyber attacks require a significant amount of near real-time reconnaissance for identifying, acquiring and impacting possible targets that, in any event, tend to change rapidly. Finally, “outsourcing” attacks may also be unattractive because of the tenuous loyalty of hackers-for-hire.

Anecdotal evidence corroborates the generally low salience of cyber security. The organizers of the conference encountered real interest on the part of CEOs, but they also detected a sense of complacency, perhaps induced by the perceived success of meeting the Y2K challenge. Cyber security does not rank among the top five of the current concerns of the CEOs of high-tech companies. Shareholders also seem quiescent. Typically, cyber security within companies is not handled at the CEO level but by information security officers (ISOs), who are mostly grouped with information officers (IOs).

Nonetheless, there is recognition on the part of many experts of the potential for major interference with, and consequent damage to, cyber networks. There is also a general apprehension about a future low-probability but high impact event. Technology may be getting better, but the increased complexity of systems may make cyber systems more vulnerable. This danger is enhanced by the fact that some criminal organizations, such as in the drugs field, have virtually unlimited access to funds. In fact, there is a curious

paradox: Optimism that the problem of cyber security can be controlled, but a foreboding that, in time, a major incident is almost inevitable. A cyber equivalent to the EXXON VALDEZ disaster, when it happens, is sure to concentrate the mind.

The issue of probability is closely connected with that of time. On the face of it, the risk of danger to cyber systems should be diminishing. Technology, such as encryption, is improving. Moreover, markets are getting better at mediating cyber risks, through insurance and controls. "Childhood diseases" are likely to be overcome. Also, while successful cyber disruption on a major scale can be done only by large, well-financed organizations and states, the likelihood of states choosing this course of action over other forms of disruption is limited. Unlike Y2K, which was a one-time event, cyber security is not a time-based problem. Whether or not we have to worry about an EXXON VALDEZ disaster down the road, the fact is that the security now in place may at some point not be enough. Markets may become less rather than more efficient because of single source software. What is required is a security management system, such as Shell has in place. It requires constant attention and updating. Making technology more secure is another constant requirement. So are security practices. These practices cannot be worked out by single industries acting alone. To be effective, they require consultation and coordination with all the actors - industry-wide and governments across national borders.

It is important to understand the nature of cyber security. It is a distributed problem. The threats come mainly from within. Parallels exist in other fields: The spy inside the FBI, the child molester who is a family member, and the restaurant employee who does not wash his hands. The challenge is to look at security as security of individuals and groups of individuals, not just as security of the state. To focus merely on the latter can lead to concentrations of power that can become dangerous. So the challenge is to reduce concentrations of power and to distribute security. Since this challenge involves everyone, and since not all people in positions of responsibility behave carefully or are trustworthy, the problem of cyber security cannot be solved. It can only be managed. Industry today copes with thousands of viruses. The challenge, as in the fields of public health and public security, is to keep cyber security problems down to levels that are considered acceptable.

Accordingly, prevailing opinion holds that the problems of cyber security can best be approached from the bottom up, and by encouraging self-reliance at neighbourhood, industry and governmental levels. Shell, for instance, has created a group-wide TCP/IP network. Better practices include openness and sharing, and the building of trust. In the international organizations area, Europol has found that it cannot effectively tackle crime committed with the use of computers without trust between that it useful, have not worked very well yet. On the other hand, the electronic crime branch of the US Secret Service has found that coordination in small groups with law enforcement, private industry and academia has worked well (New York Electronic Crimes Task Force).

A number of technical considerations affect the degree of security in the cyber world. First, much is to be said for open-source development of technology, especially software.

Reliance on a single source - such as Microsoft - carries risks; it is “against the laws of nature,” which “require diversity.” Second, it is important to reduce single points of failure, a problem the US military is addressing at each installation. Third, “server farms” need both alternate sources of energy and adequate physical security.

Government has an important role, as the guarantor of the interests of society. Government can spread information about how to use the Internet safely. It can promote R&D. It can stimulate software developers to produce security and privacy-enhancing technologies. Government can encourage the development of indicators by which users can judge company performance. Government can also provide information about what is happening on the Internet. In The Netherlands, government is trying to facilitate platforms for the exchange of information with industry, building on practices developed in preparation for Y2K.

Another key role of government and parliaments is regulation. One element is to define standards of criminal conduct. Another is to prosecute crimes, though prevention is better than prosecution after the fact. Yet another is to create rules governing liability. A functioning legal system applying rules of negligence and responsibility can function as a powerful regulator of mishap or misconduct in the realm of cyber security.

But being too dependent on government must be avoided. This American preference is increasingly shared in Europe. It is better for citizens to watch their government than to have government watch its citizens. The Soviet example, in which government is unresponsive to its citizens, and bad cases of collusion between government officials and organized crime in Russia, must be avoided. The notion of centralizing issuing authority in one central place is a bad idea. A decentralized system, that is open, transparent and not subject to possible abuse is much to be preferred. In short, there is a general preference for a distributed system.

How Should the Public and Private Sectors Work Together?

Revolutionary technical change drives cooperation. This change opens up wealth-creating opportunities. However, it also carries risks. At the macro level, key elements of the change are the growth of bandwidth and the exponential increase in speed and capacity made possible by laser technology, accompanied by the ever-lower costs of computing. At the micro level there are two developments. One is the change from the private “walled compound” computing model - in which a company buys software, customizes it, puts in a data centre behind its walls, and uses it - to so-called shared computing. In that model, companies share, on an inter-active basis, with suppliers, customers and employees a wide variety of applications, increasingly with the aid of professional hosting companies. The other development is the introduction of Internet-based packet networks. When these made their first appearance, their standards were questionable. Now these networks are moving toward quality of service guarantees. In this system, the network becomes the computer.

But as technology is moving toward open, dynamic interchange, networks become wholly business-critical and the economic risks increase. A company that opens its networks to others is at grave risk of being compromised by anybody in the outside world. Even mere denial of service or nuisance attacks can disrupt business and hurt reputations. Thus, there is increased need for security and resilience. One element is physical security of the facilities housing the machines and the software. Another element is assured security within the company, requiring good security procedures and the observance of those procedures. A third element is redundancy. “You will no longer be satisfied if you do not have at least three times redundancy of critical core corporate assets.” And last, but not least, there should be a certain dependability on transfer of data and communications across “public” information infrastructures.

Different forms of public-private cooperation have evolved in different countries. Sweden has developed a model for inclusive cooperation. It deals with IT crimes, such as viruses and fraud. It has led to the establishment of the 7799 standard which is beginning to be adopted outside Sweden as BS7799/ISO17799 based on that. It has helped companies install intrusion protection chips. This facilitates reporting of information theft. The model balances privacy with the ability to conduct internal investigations. It also provides for information sharing about better practices. The Swedish Post and Telecommunications Agency is in the lead on IT issues. Swedes accept this leading government role. This role extends into the area of national security, such as providing mobile GPS-based stations as well as extra power generators, in the context of the total defence concept. Government also leads in conducting alert exercises. This type of cooperation is based on trust through effective cooperation. The Swedish government is also involved in education and training, and funds many of these activities. They also created physically secure sites in mountains, impermeable even to

cruise missiles. All this reflects the effort to protect the Swedish Internet against intrusion. It reflects a government-industry partnership that serves Sweden well.

In the United Kingdom, we find a different model. Ineffective and dysfunctional relationships between law enforcement and industry gave rise to the creation of the Internet Crime Forum. Its membership includes the Association of Chief Police Officers, the Internet service providers, and two government departments. The Forum has reached a consensus on what are the core issues. It has come up with suggested approaches, including the allocation of costs. The size of the Forum - fifty members - has been an obstacle, but this has been met by the creation of small working groups, which report back to the Forum. One result has been a format on how law enforcement should request information and how industry should respond. Another result has been best practices guides for the provision of information and for crime prevention. The Forum has also organized case studies, involving representatives of the victim (industry), law enforcement and the prosecutor, to better illuminate and understand where the problems are. Yet other Forum initiatives have been joint training and building prevention into technology protocols.

This form of cooperation has worked well in the United Kingdom. However, poor marketing of the concept has led to a public perception that the cooperation between industry, law enforcement and government is not transparent. This problem requires further attention.

A third form of cooperation is through Information and Analysis Sharing Centres (ISACs) in the United States. Their purpose is to prevent and respond to information attacks. The Centres are set up and run by industry, and interact with government, when thought necessary. For government, they provide a point of contact to the sector. The financial service sector created an ISAC early on. Other areas are following. The Information Technology (IT) ISAC was established early in 2001. It has seventeen founding members and is open to others. Within the ISAC, competitors such as Oracle and Microsoft jointly address common problems. ISACs are a focal point of cooperation, enabling business enterprises to share proprietary and non-proprietary information, in order to prevent and respond to information attacks. Information can be introduced into this process anonymously. The work in the ISACs has not yet reached its full potential: collaboration on cyber problems is still kept down to a minimum in most sectors.

A contribution from governments on a supra-national level has been the cyber crime treaty developed by the Council of Europe and USA, Canada, Australia and South Africa. The objective is to establish a basis for international cooperation in investigation and prosecution into cyber crimes. As the information industry is concerned about attacks on computers, law enforcement is concerned with fighting crime generally, including crimes committed with the use of a computer. The challenge has been how to craft an appropriate response across borders. The Treaty constitutes such a response. However, the treaty approach raises several issues. One is that of participation in the drafting process: who is included and who is excluded. Another issue is transparency. A third is that of scope of the treaty. Moreover, the treaty approach is a slow form of creating a

regulatory system, and it should be done with caution. How the Treaty will operate will become apparent when it is ratified and enters into force. But already today its usefulness is that the new issues at hand are discussed on an international platform, and the first elements of common understanding are developed.

Finally, within the European Union (EU) several initiatives have been taken by the European Commission, very much originating from an economic perspective, where it has its mandate to operate. The EU Commission is taking into account the need for openness, transparency, the importance of focus, and the scope of the effect. For “national” security issues the Commission has no mandate: agreements on this have to be made by the European Council, which has established an office to deal with common issues on foreign and security policy. With its initiatives towards a more secure cyber space the Commission involves industry through hearings and a thorough consultation process, as it did in preparation of its Communication *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* in March 2001. In this the Commission called for the harmonisation of substantive and procedural criminal laws concerning cyber crime. Particular attention was devoted to issues such as interception of communications, retention of traffic data, anonymous access and use, practical co-operation at international level and evidential validity of computer data.

It also called for the establishment of a EU Forum on Cyber crime. Run directly by the Commission and the Joint Research Centre, this forum is expected to bring together law enforcement agencies, service providers, network operators, consumer groups and data protection authorities. Its objectives are:

- Raising public awareness on risks posed by criminals on the Internet;
- Promoting best practices for IT security;
- Developing effective counter-crime tools and procedures;
- Encouraging further development of early warning and crisis management mechanisms.

All these forms of cooperation share certain characteristics and difficulties:

- A working mix of government and industry,
- An understanding of the ramifications of IT on information security,
- Sharing of sensitive information,
- An objective-oriented approach,
- A formula for participation,
- A form of regulatory system,
- A balance between the interests of private communication with the needs of law enforcement.

These existing patterns of industry-government cooperation point to some conclusions.

First, cooperative patterns that suit one region do not necessarily suit another. Public acceptance of the Swedish model, with a predominant government role, is unlikely to work in the United Kingdom, let alone in the United States, where public distrust of government is a constitutional axiom. Effective cooperation usually starts from the ground up. It can, by example, gradually extend across borders. Top-down international regulation is subject to many pitfalls that can easily lead to failure.

Second, industry and government must face the reality that the pace of change in information technology has overtaken the ability to create walls around systems. The future is one of open sources, transparency, and open competition.

Third, ISACs depend for their effectiveness on trust and on their ability to make concrete contributions to the information society and its participants.

Fourth, the most effective initial steps are the creation of guides and best practices, to which government can make a key contribution, by offering suggestions. Governments can also create the political support needed for the effort to protect information security, to help create the organizational framework for cooperation, to assist in training, and last but not least to provide financial support where deemed in the public interest.

Next Steps for Europe

The EU Commission has recently entered the field of cyber security. On January 26, 2001, the Commission issued its first comprehensive statement. It was both a discussion paper and a policy document. On March 7, the Commission held an open hearing on the issues raised in the statement. A Forum will be established at the EU level, and have an open discussion, on-line, about cyber crime. While the Commission has not yet issued any legislative measures on cyber crime, it has done so already in earlier years in related fields, for instance on electronic commerce, data protection, and electronic signatures. It plans to issue a separate communication on network security.¹ Proposals are pending on the subjects of hacking, denial of service, copyright, and fraud with non-cash means of payment.

However, the EU approach has been cautious, and the Commission is unlikely to hurry. The Commission representative argued that there is “no real solution” to the problem of cyber crime; “we need to contain the problem.” He observed that: “we are not sure what the extent of the problem is.” The field remains surrounded by questions: How to detect intrusions when companies are reluctant to report them and how best to protect physical infrastructure. When it comes to regulation, there are questions as to what is best left to the market and what issues should be dealt with by government

The Commission considers involving the key stakeholders from the outset to be a necessary starting point. Emphasis is given to the “human element” of cyber crime by pursuing a balance between security and the creation of a “cyber space for all” respecting different societal and cultural perspectives with respect to cyber crime: encryption, privacy protection, economic priorities, and law enforcement. The growth in membership of the EU increases the complexity of this balancing act.

The issue of crime is also complex. The term cyber crime covers different criminal fields: illegal access, sabotage, espionage, and content-related crime such as pornography. But while there is general consensus that child pornography should be treated as criminal action, there is no such consensus on other issues, such as the expression of racial hatred on the Internet. Moreover, many issues are already covered by national legislation. National approaches and standards vary considerably. The Commission is still far from deciding whether it is possible or wise to attempt to harmonize a general approach to these issues, which include interception of communications, tracking and tracing, retention of data, anonymous access, searches and seizures of computers, and the evidential validity of cyber data.

Under these circumstances the EU Commission faces a Herculean task to come up with agreed definitions, measures and policy. A successful EU approach requires consultations with industry and governments at an early stage, and willingness by industry and government to listen to each other.

¹ Issued in June 2001

The Commission perspective is that many of the issues involving telecommunications are best dealt with at the “European “, i.e. EU level, even though it may be too early to think right away about legislation. Some issues, moreover, are best left to the market. The challenge, however, is to determine which are in this category.

The general feeling is that, as the Internet “market” developed in the US years before it did in Europe, the US has been facing Internet issues longer and more profound than Europe, and that thus policy making is ahead of EU decision-making. However, the importance of the Internet has been growing rapidly in Europe, too, and the EU is starting to catch up. Since its starting point for dealing with cyber crime issues is the economic perspective (related to the so called “first pillar” of the Union, i.e. economic cooperation) collaboration with industry and society has a more natural focus than having national security as a starting point, as is the case in the US. As the European approach is a much more natural basis for government – industry collaboration, rapid progress in collaboration with industry seems possible. Cooperation between the US and EU has not been fully specified yet, and suffers from the caution that comes with care for national security and/or regional economic interests. However, during the workshop it was argued that EU and US officials are satisfied with the current degree of their respective involvement in each other’s decision making process, especially in the informal discussion sessions both sides have set up for this purpose.

At the same time, however, and often implied in the discussion rather than explicitly stated, policy issues between the EU and the US did emerge:

- The general issue of privacy, where, in addition, business interests differ from government and citizens.
- The problem of data retention, where the interests of law enforcement clash with those of the telecommunications operators and Internet service providers, who could incur extra financial and litigation costs.

How Should Europe and the United States Cooperate?

The view appears to be widely held that there is a lot of cooperation across the Atlantic, between governments and among business enterprises. “All kinds of people are talking to each other all the time.” This process seems to work and “if it isn’t broke, don’t fix it.” It has many institutional settings, formal and informal: The G-8, the Council of Europe, the European Commission, the United Nations, bilateral discussions at official level, and less formal industry contacts. These venues have contributed to the creation of networks, such as among law enforcement officials. These function because they are based on professional acquaintances and trust among colleagues. Also, many of these institutional points of contact are now available seven days a week, twenty-four hours a day. It was said that it might not be a good idea to create yet more venues. They would merely add to the conferencing workload of the same set of individuals.

There appear to be no fundamental differences in practice or policy on the part of Americans and of Europeans. Of course, they cannot participate directly in each other’s regulatory functions. Nonetheless, there are many ways in which each side can hear the views of the others. This is an on-going practice that could lead, for example, to observer status on the part of the United States in EU Commission work regarding cyber security.

A key benefit of the on-going process of exchanges is increased understanding of each other’s legal and technical systems. This facilitates timely mutual legal assistance. Time is often of the essence, such as in tracking hate mail. Moreover, a system that works can be an example to other countries and move them to self-assessment and, eventually, better legislation and technology.

The Council of Europe’s Convention on Cyber Crime is an example of an effort to harmonize among 43 countries certain elements of substantive and procedural law. It points to common adoption of definitions as to what actions should be declared criminal, such as illegal access, illegal interception, data interference, and system interference such as denial of use. The Convention also seeks to extend criminal fraud provisions to computers. As to procedure, the Convention aims at adapting legal provisions and investigative powers to the computer environment.

This broad, international approach has its limits. Agreement could not be reached on the issue of liability for intermediaries. Moreover, the issue of cost in relation to retention and disclosure of data is still up to national law. Furthermore, the tendency in the laboratories remains to think in national terms. At heart, the information technology world is still very much a bottom-up phenomenon. “It is very much like grass growing.” People resist technical standardization for reasons relating to competition and innovation. Thus, as Ambassador Schneider pointed out, the problems are global, but the answers are still to a large degree national or regional.

In this context, there are issues that do not get an agreed global response, such as where to strike the balance between the use of encryption technologies and the needs of law enforcement. This is an area that in many countries lacks a sound legal basis. This situation creates problems for multinational companies, which face diversity of legal regulation when doing business in many countries. Thus, sharing experiences and educating consumers are well worth the effort. Nonetheless, there are certain issues, such as data retention, which ought to be tackled at the international level, complicated as this may be.

In sum, there is a solid consultative network in place, but each state has a different way of consulting with industry, so in the end there is a patchwork of how global industries feel they have been consulted. As a result, industry on some issues speaks with more than one voice. Furthermore, governments and parliaments also have their national perspectives. So we are seeing a very distributed discussion, both at the national and at the international level. All this warrants further efforts at information sharing to achieve a kind of overview on the status of different elements, such as dependability of information structures. It is therefore very timely the Commission is supporting the Dependability Development Support Initiative, a European project with exactly these aims (www.ddsi.org).

Challenges/Suggestions

Understanding the Problem

We have entered a new phase of technological change. But “there isn’t even a beginning of understanding” of all the issues relating to the protection of cyber security. The speed of technological change overtakes considered planning. Legislation cannot catch up with changing technology. “The legal and political people have backward-looking mirrors on their head, and they compare everything they see with what was done in the past 200 years. But we see new things all the time.”

We have not completed the transition to digital technology. Nor have we yet adopted common terminology. We are facing all sorts of non-traditional financial transactions. We do not fully understand the implications of cyber security on data privacy. And we have only seen the beginning of a discussion about these issues across industries and among governments. Key to dealing with the phenomenon is perhaps not to try and govern it, but to enable it and provide a framework for the public and private sector to learn by doing and best practices.

Technical Requirements

Industry must insist on secure and trustworthy hardware and software and more dependable technology. Standards are an important in this - indeed indispensable - tool for enhancing cyber security: Access protocols, authentication certificates and security procedures. By preference these should be based on open source, rather than a single closed source (like Microsoft). It is far preferable to have a multiplicity of issuing authorities.

The Trust Issue

Trust presents a paradox. On the one hand, trust is an essential element of effective cooperation. Europol, for instance, cannot be effective without trust from the private sector and from counterparts in other countries. ISACs cannot function without mutual trust. Industry expects government not to harm its business interests inadvertently. The FBI counts on business to report the information it needs to do its job. So trust is a key element in dealing with cyber security and related crime.

On the other hand, misplaced trust can lead to serious trouble. The cyber security field is littered with examples of the damage that can be done by insiders (compare, in other contexts, the Ames case at CIA and the Hansen case at the FBI). Thus, there is an inescapable requirement for due diligence in the commercial field, and of proper security practices - such as password protection and reliable authentication procedures - that are applied and consistently followed.

Thus, in protecting cyber systems and practices, the trust issue remains an element of tension that requires the thoughtful application of good judgment.

Additional Players

There are a number of potential actors who could play key roles but are not yet fully engaged.

- Software vendors. Customers will pressure them for more reliable software and a transparent market.
- Insurance companies. As in the field of health care, their focus will be on prevention.
- Auditing firms. There is a role for them in making judgments about IT industry practices and procedures.
- Stock markets. Markets and their regulatory authorities have an interest in transparency of cyber security vulnerabilities of listed companies.
- Issuers of certificates of authentication. These companies, such as Verisign and Microsoft, play a decisive role in validating the authenticity, use, and credibility of their certificates.
- Security departments and companies. This sector of business is growing fast, spurred by the Y2K experience.

Regulation

First comes creation of an organized mechanism for cooperation. Next, the process should be open to all potential participants. The scope of the process must be adequate; it should encompass security as well as crime. The focus of regulation, though, needs to be narrow. The objective should be viable economic models that balance the interests of industry, government and citizens. Best practices are a good first step. Throughout, habits of cooperation are essential.

Legislation

Government can put order into the discussion and treatment of cyber security issues. In addition, it has a powerful regulatory function. Laws will have a tough time keeping up with technological changes affecting cyber security. But commercial law, in particular, must attempt to keep up with practical problems, such as digital signatures, the use of encryption, and the issue of liability.

Criminal law, being a heavy tool, should be formulated with caution, preferably awaiting the effect of new technologies. A model for penalty handling could be based on or at least include lawsuits related to economic damage. Every effort should be made to draft legislation so it does not go out of date. Meanwhile, government can act in the areas of self education, training, preventive measures, readiness, early warning alert systems, all in consultation with industry.

Law Enforcement

Criminal justice cannot be applied effectively to cyber crime absent disclosure by injured parties to law enforcement authorities of the circumstances of their losses. Such disclosure is tightly linked to trust that putting a company's losses into the public domain will not lead to further, competitive losses. Voluntary industry associations, such as ISACs, and a base of experience in this nascent area can help establish that trust. Law enforcement must learn to apply shared information selectively.

Subsidiarity

The conclusion was that it is wise to avoid attempting to legislate and regulate at the highest level. The best approach is to start at the lowest levels and work from the bottom up. The ISAC in the US financial industry set the example for other industries. Regional umbrella organizations work best when all members provide input and when they produce concrete and practicable suggestions. A national approach that is shown to be useful may be ripe for international application. A national business organization, however, may be hampered because not all industries are represented, because its members will have the usual difficulty in arriving at policy positions, or because they have done a poor job explaining their purpose. But some, like the Swedish Trade and Industry Delegation, have been effective. So has the EU Directive on Distant Services. In addition to centralizing the discussion on cyber security among EU members, the Commission is being instrumental in helping member states set up national systems.

Strengthening the Cyber Security Community.

The successes, such as they are, of coping with cyber security problems is due in large measure to the existence of an increasingly global community of experts, in government, industry and academia. The organizational structures created for dealing with cyber security forms a useful skeletal framework for cooperation. However, much of the effectiveness of the cyber security community is due to informal contacts and networking. Creating more venues is not the answer; this approach would simply add to the busy conference schedules of the same set of experts. But much is to be gained by widening the public debate. The April 9 conference and this report are contributions to that objective.

=O=

Annexes

Annex 1 – Conference Agenda

Cyber Security: What Does the Private Sector Expect from Governments?
A Transatlantic Perspective

Conference co-organized by the US Embassy in The Hague and RAND Europe
The Hague, April 9, 2001

- 0845 - 0900 Introduction
H.E. Cynthia P. **Schneider**, U.S. Ambassador to the Netherlands
Alan **Matula**, Royal Dutch/Shell
Bouke **Veldman**, RAND Europe
- 0900 - 0945 Keynote: Esther **Dyson**, EDVenture Holdings
- 0945 - 1115 Framing the question. What are the threats and what is the matrix of possible responses? – Chairman: Marten **van Heuven**, RAND Europe
Robert **Anderson**, RAND
Pieter **Van Dijken**, Shell Services International
Paulo **Felix**, Europol Intelligence Analysis Department
Guus **Broesterhuizen**, Netherlands Ministry of Transport
- 1115 - 1130 Coffee break
- 1130 - 1300 How should the public and the private sector work together? – Chairman:
Jack **McMaster**, KPNQwest
Fredric **Sand**, Swedish Cabinet Office
Keith **Akerman**, Chair, U.K. National Computer Crime Working Group
Jeffrey F. **Pryce**, Steptoe & Johnson
- 1300 - 1400 Lunch
- 1400 - 1445 Next Steps for Europe: Rogier **Holla**, European Commission
- 1445 – 1615 How should Europe and the United States cooperate? – Chairman: Haico **Meijerink**, Cisco Systems International BV
Betty **Shave**, U.S. Department of Justice
Alexander **Patijn**, Netherlands Ministry of Justice
Armgard **von Reden**, IBM
- 1615 - 1630 Coffee break
- 1630 - 1730 Open Discussion – Chairman: Paul **de Graaf**, VNO-NCW
- 1730 Drinks

Annex 2 – List of Participants

Name			Organisation	Country
Mr.	K.	Akerman	Hampshire Constabulary	United Kingdom
Ms.	Diana M.	Alonso Blas	Registratiekamer	The Netherlands
Mr.	Robert H.	Anderson	RAND	USA
Ir.	Jaap W.J.	baron van Till	Stratix Consulting Group B.V.	The Netherlands
Mr.	Joost	Batelaan	DutchTone	The Netherlands
Mr.	Maarten	Botterman	RAND Europe	The Netherlands
Dr.	G.A.A.M.	Broesterhuizen	Directorate General Telecommunications and Post	The Netherlands
Mr.	Michael A.T.	Cooper	Het Financieele Dagblad	The Netherlands
Dr.	Paul W.J.	de Graaf	VNO NCW	The Netherlands
Mr.	Stephen	De Spiegeleire	RAND-Europe	The Netherlands
Ms.	Barbara	di Turi	ABN-Amro Bank	The Netherlands
Professor	Wim	Dik	Delft University	The Netherlands
Mr.	James M.	Dorsey	The Wall Street Journal Europe	The Netherlands
Ms.	Esther	Dyson	Edventure	USA
Ir.	G.	Ekkelenkamp	TU/e (Technische Universiteit Eindhoven)	The Netherlands
Dr.	Paulo	Felix	Europol	The Netherlands
Dr.	Alexander	Galitsky	TrustWorks Systems	The Netherlands
Ms.	Carlanda L.	Hassoldt	American Consulate General	The Netherlands
Mr.	Rogier	Holla	European Commission, Information Society Directorate-General	Belgium
Mr.	Anton	Holleman	Origin B.V.	The Netherlands
Prof. Dr.	A.B.	Hoogenboom	Ernst and Young Forensic Services	The Netherlands

Managing New Issues: Cyber Security in an Era of Technological Change

Dipl. Ing.	Reinhard	Hutter	IABC	Germany
Mr.	Sergej	Katus	Federatie Nederlandse IT	The Netherlands
Ir.	P.W.J.	Kornelisse	KPMG	The Netherlands
Mr.	Philip S.	Kosnett	Embassy of the United States of America, The Hague	The Netherlands
Mr.	Eric	Luijff	TNO Physics and Electronics Laboratory	The Netherlands
Mr.	Alan	Matula	Royal Dutch/Shell	The Netherlands
Mr.	Jack	McMaster	KPNQwest	The Netherlands
Mr.	Haico H.J.	Meijerink	Cisco Systems International B.V.	The Netherlands
Mr.	Stanely W.	Milo	Roccade Megaplex	The Netherlands
Mr.	Frans-Jan	Mulschlegel	Europol	The Netherlands
Mr.	O.	Olofsen	Fortis Bank	The Netherlands
Mr.	Alexander	Patijn	Ministry of Justice	The Netherlands
Ms.	Angier M.	Peavy	Embassy of the United States of America, The Hague	The Netherlands
Mr.	Jeffrey F.	Pryce	Step toe and Johnson, LLP	USA
Mr.	Jan	Razoux-Schultz	Embassy of the United States of America, The Hague	The Netherlands
Ir.	Appie A.J.	Reuver	IBM Nederland N.V.	The Netherlands
Mr.	G.A.J.	Rijgwart	VNO NCW	The Netherlands
Mr.	Peter	Roelse	TU/e (Technische Universiteit Eindhoven)	The Netherlands
Mr.	Fredrik	Sand	Ministry of Industry, Employment and Communications	Sweden
Ambassador	Cynthia P.	Schneider	Embassy of the United States of America, The Hague	The Netherlands
Ms.	Betty-Ellen	Shave	U.S. Department of Justice	USA
Mr.	Michael A.T.	Spector	The New Yorker	Italia
Mr.	Don	Taylor	Dow Benelux N.V.	The Netherlands
Mr.	Bob W.	Toetenel	Getronics	The Netherlands

Mr.	Mark A.	Tokola	Embassy of the United States of America, The Hague	The Netherlands
Mr.	Lorenzo	Valeri	International centre for Security Analysis, King's College London	United Kingdom
Mr.	Peter	van Ammelrooy	de Volkskrant	The Netherlands
Ing.	C.C.	van den Brink	AKZO Nobel	The Netherlands
Mr.	Ronald	van der Luit	Directorate General Telecommunications and Post	The Netherlands
Mr.	W.F.	van der Most van Spijk	KLM Royal Dutch Airlines	The Netherlands
Mr.	Pieter	van Dijken	Shell Service Internationa B.V.	The Netherlands
Mr.	Robert	van Eijl	OPTA	The Netherlands
Dr.	A.J.P.M.	van Gessel	Fortis Bank	The Netherlands
Mr.	Marten	van Heuven	RAND Europe	USA
Mr.	Bouke	Veldman	RAND Europe-Leiden	The Netherlands
Drs.	Henk Jan	Vink	TNO Fysisch en Elektronisch	The Netherlands
Ms.	Armgard	von Reden	IBM Brussels	Belgium
Drs.	Richard H.P.	Vriesde	Politie Haaglanden	The Netherlands