

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

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.