Statement of

LANCE J. HOFFMAN

Professor, The George Washington University

before the

U. S. Senate Committee on Commerce, Science, and Transportation

June 10, 1999

My name is Lance J. Hoffman. I am a professor in the Department of Electrical Engineering and Computer Science at The George Washington University in Washington, D. C. I also am Director of the School of Engineering's Cyberspace Policy Institute and the author or editor of five books and numerous articles on computer security and privacy. My most recent book is a compendium of papers on the encryption policy problem entitled *Building in Big Brother* (Springer-Verlag, New York, 1995).

Currently, I am the principal investigator for a project entitled "Cryptography Products and Market Survey". As part of that project, we have recently produced a report entitled "Growing Development of Foreign Encryption Products in the Face of U. S. Export Regulations". I am leaving you copies of that report, which is also available from the Institute or on our Web site at http://www.seas.gwu.edu/seas/institutes/cpi/library/papers.html, where detailed tables and charts supporting this testimony are also available. We did this work in cooperation with NAI Labs, the Security Research Division of Network Associates, Inc., Glenwood, Md. The project manager for NAI Labs, Mr. David Balenson, is with me today. We were assisted in this project by three students.

In the project, we surveyed encryption products developed outside the United States and found that the **development of cryptographic products outside the United States is not only continuing but is expanding to additional countries; with rapid growth of the Internet, communications-related cryptography especially is experiencing high growth.**

As of June 8, 1999, **we identified 805 hardware and/or software products incorporating cryptography manufactured in 35 countries outside the United States.** As shown in Attachment 1, the greatest number of foreign cryptographic products are manufactured in the United Kingdom, followed by Germany, Canada, Australia, Switzerland, Sweden, the Netherlands, and Israel in that order. Other countries accounted for slightly more than a quarter of the world's total of encryption products.

These 805 foreign cryptographic products represent a 149-product increase (22%) over the most recent previous survey in December 1997. At least 167 of them use strong encryption, the kind that one cannot export from the United States without applying for and receiving export license approval. The algorithms used in these are Triple DES, IDEA, BLOWFISH, CAST-128, or RC5.

Cryptography product manufacturers have appeared in six new countries since December 1997: Estonia, Iceland, Isle of Man, Romania, South Korea, and Turkey. **There has also been a large increase in the number of products produced by** certain countries**.** The **United Kingdom** jumped by 20 products from 119 to 139, and **Germany** jumped from 76 products to 104. Also notable was **Japan**'s increase, from six products to 18, and **Mexico**'s, from a single product to six.

There are now 512 foreign companies that either manufacture or distribute foreign cryptographic products in 70 countries outside the United States. Attachment 2 lists these countries.

On average, the quality of foreign and U. S. products is comparable. We have encountered poor products both within and outside the U.S., and we have encountered good products both within and outside the U.S. There are a number of very good foreign encryption products that are quite competitive in strength, standards compliance, and functionality.

A significant number of foreign competitors to U.S. manufacturers of software and hardware with encryption capabilities are developing products with strong encryption, and have as customers a number of large foreign or multinational corporations. The report gives thumbnail sketches of some of these companies and their offerings.

We found some examples of advertising used by non-U. S. companies that generally attempted to create the perception that purchasing American products may involve significant red tape and the encryption may not be strong due to export controls. As an example, we show in Attachment 3 material from Cybernetica's Web site in Estonia. We give several other examples of similar advertising in the report.

Companies want to sell encryption products that meet certain accepted worldwide standards. Encryption experts from all over the world have contributed to two important international standards efforts, IPsec and the Advanced Encryption Standard. In the case of IPsec, there are currently implementations (complete or in the works) from at least nine companies in five foreign countries. One effort, the KAME Project, is a joint effort of several Japanese companies (Fujitsu, Hitachi, IIJ Research Laboratory, NEC, Toshiba, and Yokogawa).

In 1997, the National Institute of Standards and Technology (NIST) solicited algorithms for the Advanced Encryption Standard (AES) to replace the Data Encryption Standard (DES) as a U. S. government encryption standard. Individuals and companies from eleven different foreign countries proposed 10 out of the 15 candidate algorithms submitted to NIST. So it is very possible that the next U.S. government encryption standard will have been designed outside the United States. Details on who submitted what algorithm are given in Attachment 4.

Finally, our empirical product data could be combined with economic measures and economic theories to better explain why we are seeing the observed growth in the

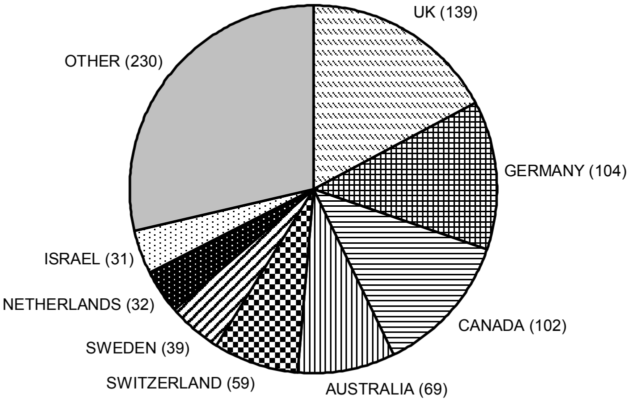
cryptography marketplace, and to examine the effects of Internet growth, e-commerce development, and regulatory actions on the international cryptographic market over time, thus getting better insights into the implications of various policy options. We should be able to combine previous work with studies already available on the information technology sector and the data in our study to better understand the changes we are seeing in the global marketplace, and thus be able to more easily adjust national laws for a global economy.

Attachment 1. Foreign Cryptographic Products by Country

Foreign Cryptographic Survey Results (as of May 1999)

The updated survey identified a total of 805 foreign cryptographic products from 35 countries:

Argentina
Australia
Austria
Belgium
Canada
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hong Kong
Iceland
India
Iran
Ireland
Isle Of Man
Israel
Italy
Japan
Mexico
Netherlands
New Zealand
Norway
Poland
Romania
Russia
South Africa
South Korea
Spain
Sweden
Switzerland
Turkey
UK



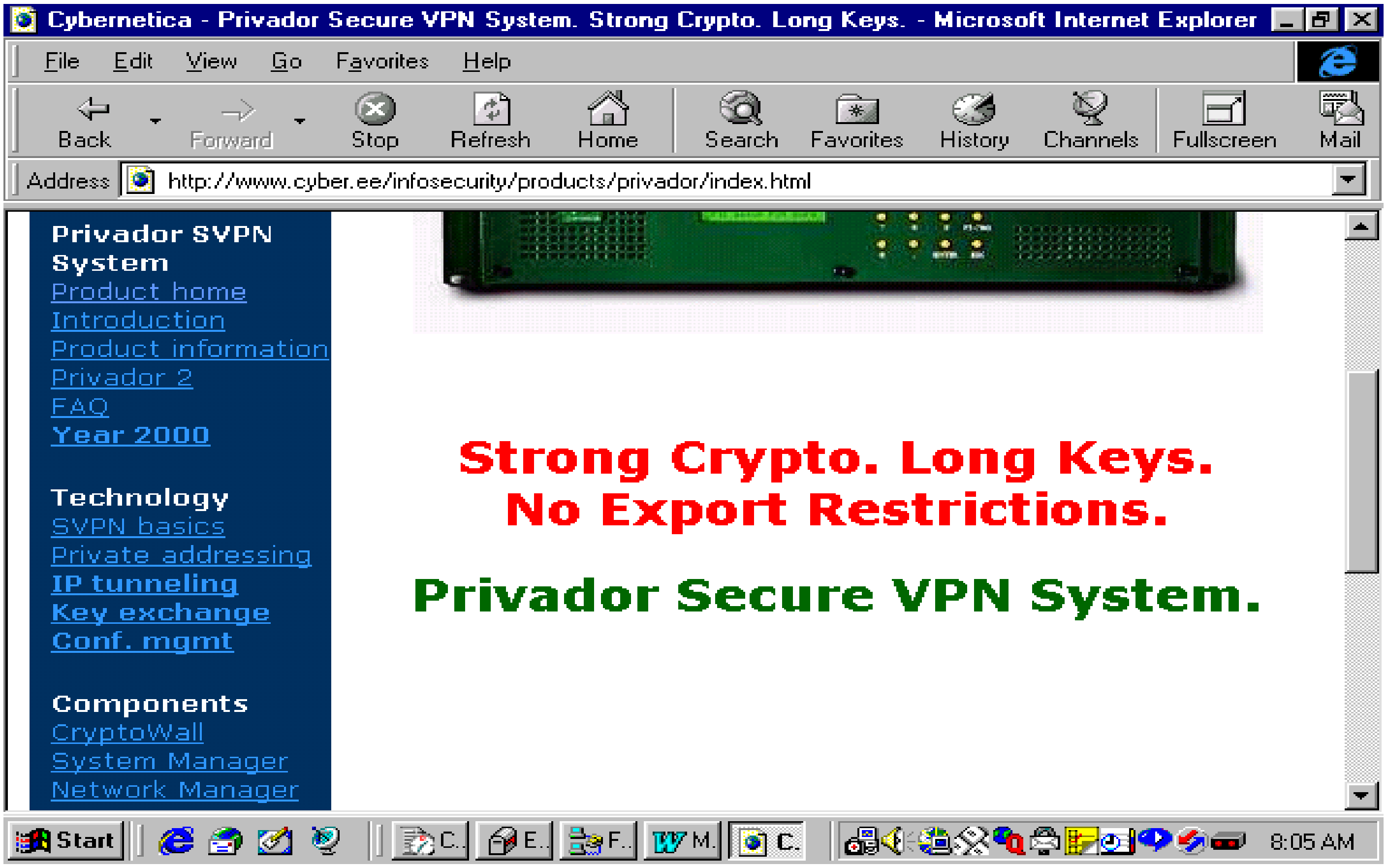
At least 167 of these foreign cryptographic products implement "strong" cryptographic algorithms, including Triple DES, IDEA, BLOWFISH, RC5, or CAST.

We identified 512 foreign cryptography companies (including distributors as well as manufacturers) in 70 countries.

Attachment 2. Foreign countries in which cryptography is manufactured or distributed

Argentina
Australia
Austria
Bahrain
Baltic Republics
Bangladesh
Belgium
Brazil
Brunei
Canada
Chile
Colombia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Ghana
Greece
Hong Kong
Iceland
India
Indonesia
Iran
Ireland
Isle of Man
Israel
Italy
Ivory Coast
Japan
Kenya
Kuwait
Luxembourg
Madagascar
Malaysia
Malta
Mauritius
Mexico
Nepal
Netherlands
New Zealand
Nigeria
Norway
Oman
Philippines
Poland
Portugal
Qatar
Reunion
Romania
Russia
Saudi Arabia
Singapore
Slovak Republic
South Africa
South Korea
Spain
Sweden
Switzerland
Taiwan
Thailand
Turkey
United Arab Emirates
United Kingdom
Venezuela
West Indies
Yugoslavia
Zimbabwe

Attachment 3. Example of advertising used to create a perception that
American products = red tape and weak encryption



Cybernetica - Privador Secure VPN System. Strong Crypto. Long Keys. - Microsoft Internet Explorer

Address http://www.cyber.ee/infosecurity/products/privador/index.html

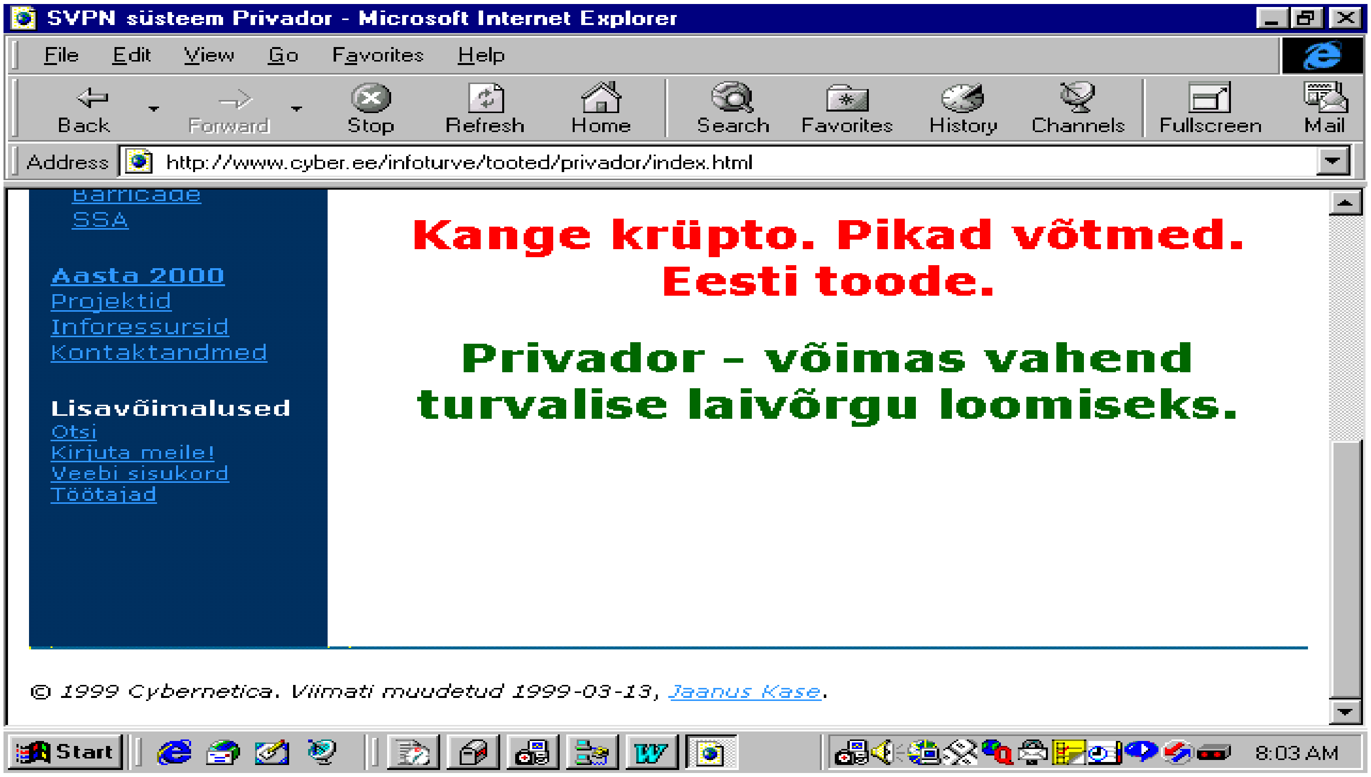
Privador SVPN System
Product home
Introduction
Product information
Privador 2
FAQ
Year 2000

Technology
SVPN basics
Private addressing
IP tunneling
Key exchange
Conf. mgmt

Components
CryptoWall
System Manager
Network Manager

Strong Crypto. Long Keys.
No Export Restrictions.

Privador Secure VPN System.



SVPN süsteem Privador - Microsoft Internet Explorer

Address http://www.cyber.ee/infoturve/tooted/privador/index.html

Barricade
SSA

Aasta 2000
Projektid
Inforessursid
Kontaktandmed

Lisavõimalused
Otsi
Kirjuta meile!
Veebi sisukord
Töötajad

Kange krüpto. Pikad võtmed.
Eesti toode.

Privador - võimas vahend turvalise laivõrgu loomiseks.

© 1999 Cybernetica. Viimati muudetud 1999-03-13, Jaanus Kase.

Attachment 4. Proposed Candidates for Advanced Encryption Standard

Country	**Candidate Algorithm**	**Submittor(s)**
Australia	LOKI97	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry
Belgium	RIJNDAEL	Joan Daemen, Vincent Rijmen
Canada	CAST-256	Entrust Technologies, Inc.
	DEAL	Outerbridge, Knudsen
Costa Rica	FROG	TecApro Internacional S.A.
France	DFC	Centre National pour la Recherche Scientifique (CNRS)
German	MAGENTA	Deutsche Telekom AG
Japan	E2	Nippon Telegraph and Telephone Corporation (NTT)
Korea	CRYPTON	Future Systems, Inc.
USA	HPC	Rich Schroeppel
	MARS	IBM
	RC6	RSA Laboratories
	SAFER+	Cylink Corporation
	TWOFISH	Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson
UK/Israel/Norway	SERPENT	Ross Anderson, Eli Biham, Lars Knudsen

Smid, M., and M. Dworkin, Special Report on the First AES Conference, presented at Crypto '98 Conference, August 1998, http://csrc.nist.gov/encryption/aes/round1/crypto98.pdf.