Cybercrime
Research Institute

STEIN SCHJOLBERG

THE HISTORY OF CYBERCRIME

THIRD EDITION

VOLUME 13

”It is no longer a question of a nation protecting its own security, it is a question of the global community protecting itself.”

Kapil Sipal
Minister for Communication and Information Technology
India (2012)

To
FBI for guiding me to the knowledge of computer crime, and

INTERPOL that let me open up the global combat, and

ITU for searching for a global common ground on cybersecurity,

And

In the Memory of Professor Jon Bing, University of Oslo

PREFACE AND ACKNOWLEDGEMENT

Senator Joseph R. Biden Jr.
Senator Richard G. Lugar:

June 1, 2006

30 years anniversary for the Ribicoff Bill

The Ribicoff Bill was introduced to the 95th Congress, First Session, in May 1977 as S.1766 the ”Federal Computer Systems Protection Act of 1977.”

The Bill was not enacted as law, but this pioneer Bill created an awareness and guidance for national legislations around the world. It was the beginning of a new age for law enforcement and legislations, the computer age.

Senator Biden described it in the closing remarks of his opening statement at the hearing on June 21, 1978 as follows:

”First we turn to the distinguished senior senator from Connecticut who deserves a great deal of credit for hearing those voices in the wilderness and focusing the

Senate´s and this committee´s attention on the crime of the future –computer crime.”

I visited the Senate in 1978 and learned of the Bill and has since been involved with computer crime laws and cybercrime laws, both on national and international level.

The Ribicoff Bill was of great importance to all of us working with this subject in the early stage of the legal development, and I suggest that the Bill should deserve a celebration on the 30 years anniversary in 2007.

Best regards

Stein Schjolberg
Chief Judge
Moss tingrett Court
Norway
www.cybercrimelaw.net

My interest in computer crime started in 1976 when I visited USA on a study tour organized by FBI. My visit included also a meeting at the US Department of Justice, where I was introduced to the new phenomenon “computer crime” at a meeting with Nathaniel E. Kossack, Deputy Assistant Attorney General, Criminal Division, US Dept. of Justice. I made a report to the Norwegian Ministry of Justice in November 1976.

I was also associated with Professor Jon Bing, the Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo, on a research project on computer crime under a grant from the Norwegian Ministry of Justice.

This cooperation resulted in 1977 in seminars in Stockholm, Copenhagen and Oslo, in collaboration with the police and University authorities in the Scandinavian capitals.

Another study tour to the US Department of Justice, US Senate, and many FBI offices around the United States was made in 1978. The Faculty of Law, University of Oslo, published the report.

The round trip to the FBI offices around United States in 1976 and 1978 was organized by Special Agent Dennis Dickson, then Assistant Legal Attache, US Embassy, London, United Kingdom.

I was then invited as a speaker at the 3rd INTERPOL Symposium on International Fraud in Paris and was one of individuals that introduced INTERPOL to computer crime.

I am deeply grateful to all individuals and institutions mentioned above in these pioneer years.

A special thanks for the cooperation and assistance in the recent years is addressed to Professor Solange Ghernaouti, Switzerland, and CEO Graham Butler, United Kingdom. They were members of the global High-Level Experts Group (HLEG), at ITU, Geneva, and from 2013 have joined me as members of the ThinkTank “Peace, Justice and Security in Cyberspace”.

Another special thanks goes to Secretary-General Hamadoun Toure, ITU, that appointed me as the Chairman of HLEG.

A special thanks is also addressed to professor Marco Gercke, Germany, for all his support and assistance.

I am deeply grateful to my wife Aasa, and my sons Kai and Rune that have assisted me in my work throughout the years.

The following book is a brief introduction to the history of the legal framework for combating computer crime, and as it later has been termed “cybercrime”.

Foreword on the Second edition (2016)

In 2016 I celebrate 40 years of research on computer crime and cybercrime from 1976 until 2016. My basic research was developed at the Norwegian Research Center for Computers and Law, Faculty of Law, University of Oslo, and at the SRI International (Stanford Research Institute), Menlo Park, California, USA.

In the Second edition I have updated the book with the global developments in cyberspace issues since 2014, on cybersecurity and cybercrime. The developments of Internet of Things (IoT), criminal conducts in social media, and public-private partnerships for the investigation of cybercrime, are especially important to follow. The very serious terrorist attacks have revealed that law enforcements access to encrypted communications have been a great problem, even with a Court Order.

A Global Convention or Declaration for Cyberspace is clearly needed as a framework on cybersecurity and cybercrime, and as a contribution for peace, security and justice in Cyberspace.

I am deeply grateful to Professor Marco Gercke, Germany, for all his assistance and making this book in a Second edition.

March 2016

Stein Schjolberg

Foreword on the Third edition (2019)

In the Third edition I have updated the book with the global developments in cyberspace issues on cybersecurity and cybercrime since 2016. Many important declarations and statements have been made the last two years. But there have not been any developments on binding global norms and regulations on the United Nations level. Without any consensus, the global situation may be described as polarized.

Today the developments of the global IT companies such as Google, Facebook, Apple, Amazon, and Microsoft, have been so rapid and the impact on the global society the last 6-7 years enormous, without developing any international regulations and guidelines for cyberspace.

It may be argued that the global private IT companies have now been the leading organisations on global Internet governance, instead of United Nations organisations.

The rapid growth of cyberspace has created new developments for online vulnerabilities and cyberattacks on the critical information infrastructures of sovereign States. The global cyberattacks may even constitute a threat to international peace and security and need a response in global regulations and guidelines in a global framework to promote peace, security and justice, prevent conflicts and maintain focus on cooperation among all nations. Dialogues and cooperation between governments on norms and standards in cyberspace must best be achieved through a United Nations framework. Regional and bilateral agreements may not be sufficient.

The principles of State sovereignty must also apply in cyberspace. States enjoy sovereignty over any cyber infrastructure located on their territory and activities associated with that cyber infrastructure.

A proposal for a United Nations Convention or Declaration for Cyberspace may today be described as a search for a common ground.

I am deeply grateful to Professor Marco Gercke, Germany, for his continuesly assistance and making this book in a Third edition.

I made a closing statement in my presentation at United Nations World Summit on the Information Society (WSIS) Forum 2018, Geneva, March 19-23, 2018, as follows:

I pray that USA and China will reopen again their excellent High-level Joint Dialogues, that was held every second time in Beijing and Washington DC, last time in December 2016. And in adition invite Russia to participate in the dialogues.

December 2019

Stein Schjolberg

Index

1. INTRODUCTION

1.1 A presentation of the book

This book presents the history of computer crime and cybercrime from the very beginning with punch cards, to the current data in the clouds and the Internet of Things (IoT).

Since the first introduction of computer technology to governmental operations and the private sector in the 1970-ties, criminals have also found and exploited weaknesses in the technology.

Individual pioneers, especially in the United States, recommended from the late 1970-ties a need for updating existing criminal laws to include the technological innovations. This book presents the great early efforts by various computer crime experts, when private personal use of computer technology was still in the early stages of the growth curve. Even these early efforts recognized the potential for globalization of some categories of malicious behaviors and recommended that States should come together and to create compatible laws and investigative cooperation.

The text that follows this introduction provides also a brief history of these computer experts and their recommendations.

The first comprehensive initiative on proposals for new computer crime legislation was the Ribicoff Bill in the United States in 1977, presented by Senator Abe Ribicoff. This Bill created awareness around the world as to the potential problems that unauthorized computer usage could cause, and the need to define the scope of the topic in order to

adequately address the problems in a comprehensive but flexible way.

This book then introduces an overview over the pioneer States that followed the recommendations in the 1980-ties.

The pioneer period of individuals and States may be considered as ended with the introduction of the first recommendations from the regional organizations in 1989. But INTERPOL was the first international organization that initiated information and discussions on computer crime in 1980/81 and it was followed up by the OECD guidelines on judicial measures.

The first comprehensive recommendation was presented in 1989 by The Council of Europe Recommendation on Computer-related crime. From then on the regional international organizations took the lead, and presented the guidelines that the States were recommended to follow.

The book presents the guidelines for computer crime legislation from the regional organizations in the 1990-ties and later on.

From the year 2000 the global organization of United Nations participated in the developments, also as leading organizations in the development, through United Nations organizations such as the International Telecommunication Union (ITU) in Geneva, and the United Nations Office for Drug and Crime (UNODC) in Vienna.

Cyberspace[1] as the fifth common space, after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. It is necessary to make the international community aware of the need for a global response to the urgent and increasing cyber threats. The international guidelines from 2000 and thereafter introduced the term ”cybercrime”.

Today the technological development of social media, such as Google, Facebook, YouTube, Twitter, and more, have been so rapid and the impact on society so fast and enormous, that codes of ethics, and public sentiments of justice implemented in criminal legislations, have not kept pace. Conducts in social media need a better protection by criminal laws. But with the reluctance in developing similar responses in international laws or guidelines, we must ask ourselves if we once again may be in a similar situation as the US Senator Ribicoff focused on in 1977:

Our committee investigation revealed that the Government has been hampered in its ability to prosecute computer crime. The reason is that our laws, primarily as embodied in title 18, have not kept current with the rapidly growing and changing computer technology.

Consequently, while prosecutors could, and often did, win convictions in crime by computer cases, they were forced to base their charges on laws that written for purpose other than computer crime.

Prosecutors were forced to "shoe horn" their cases into already existing laws – when it is more appropriate for them to have a statute relating directly to computer abuses.

Governments, private industry and the global society are relying upon continuous availability and integrity of information and communications infrastructures. Maintaining the confidentiality, integrity, and availability of the cyber networks and the data they carry, increases the trust the global community place in the information and communication infrastructures. Only through developing compatible standards and laws can such innovation continue to grow. How we shape standards and legal norms of conduct today will affect the future growth in technology and innovations.

Cyber attacks against critical information infrastructures of sovereign States, must necessitate a response for global solutions. I assume that most of the judges and lawyers around the world from a professional judicial point of view, agree with the former US prosecutor Benjamin B. Ferencz in his statement:

There can be no peace without justice, no justice without law and no meaningful law without a Court to decide what is just and lawful under any given circumstances.

The problem of establishing International Courts or Tribunals is thus a political or geo-political decision, and not a professional judicial question.

1.2 The development of the Internet

Internet as we know it today has its background in a Network called “ARPANET” in 1968 when the first experimental network was built. A research group at the Network Information Center (NIC) in the United States electronically connected their computer to another computer at the University of California in Los Angeles (UCLA) and started the ARPANET.[2]

On October 29, 1969, two programmers in California, 400 miles apart, successfully sent a message between the two different institutions, University of California, Los Angeles (UCLA) and Stanford Research Institute (SRI). UCLA and SRI became the two first functional nodes of the ARPANET.

The development of (Advanced Research Projects Agency Network) ARPANET was described by FBI at the hearing in United States Congress in 1994[3] as a government experiment. The research project linked researchers with remote computer centers, allowing them to share hardware

and software resources such as computer disk space (storage), databases, and computing power.

The original ARPANET was began by the U.S. Department of Defense Advanced Research Projects Agency (ARPA)[4] as a US military program, which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the Network were damaged in a war.[5] The original ARPANET was then split into two networks the ARPANET and the MILNET, a military network. These two networks were allowed the exchange of information to continue.

The international development of ARPANET was established in 1973, when Norway[6] and United Kingdom became the two first functional international nodes.

Cooperative decentralized networks such as UUCP, a worldwide UNIX communications network, and USENET, users network, were introduced in the late 1970-ties initially serving the University community and later commercial organizations. In the beginning of 1980-ties, networks such as the computer science network (CSNET) and BITNET were developed serving network capabilities to the academic and research communities. Special connections were then developed to allow exchange of information between various communities. The National Science Foundation Network (NSFNET) was introduced in 1986, and linked researchers across United States with five supercomputer centers. NSFNET expanded the following year including more networks that were linked to more universities and research centers, and started to replace ARPANET that was closed down in March 1990. In 1994 it was expanded worldwide and made up of around 30.000 interconnected computer networks.

NCSA Mosaic, or Mosaic,[7] was the web browser that laid the foundation of popularizing the World Wide Web. It was developed at the National Center for Supercomputing Applications (NCSA) in the United States,[8] and the browser was released in 1993. Mosaic was also the first browser to display images inline with text instead of displaying images in a separate window.

Netscape Navigator[9] was developed by Netscape Communications Corp in the United States and released in December 1994. It became the dominant web browser until 2000, when Microsoft's Internet Explorer became the dominant web browser. The development of Netscape Navigator was stopped in December 2007 but became the basis for Mozilla Firefox. The Internet was in the 1990-ties commonly called "The Information Superhighway."

United States Supreme Court made the following evaluation of the Internet in a Court opinion in 1997:[10]

The dramatic expansion of this new marketplace of ideas contradicts the factual basis of this contention. The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship.

---

[1] Although now ubiquitous in usage, the term cyberspace used to denote both the social and physical networks that make up the Internet as a unique space distinct from non-networked world, did not enter in the English lexicon until 1982. The term was coined by the Canadian science-fiction author William Gibson in his 1982 short story "Burning Chrome" but was ultimately launched into popular usage by his 1984 novel "Neuromancer" and the word became identified with online computer networks, see Wikipedia and Professor Lawrence

Lessig, Stanford Law School, Stanford University, USA: ”Code and Other Laws of Cyberspace”, page 5 (2000), and howtogeek.com

[2] SRI Alumni Association, December 2009, April 2012 Newsletter page 4.

[3] Testimony by Thomas T. Kubic, Chief Financial Crimes Section, FBI, before the Subcommittee on Science, on March 22, 1994.

[4] ARPA was established by President Eisenhower in 1957. Researchers at MIT and Stanford Research Institute (SRI) were the main researchers on this project.

[5] See: Justice Stevens delivered the opinion of the Court in United States Supreme Court Case No. 96-511, June 26, 1997.

[6] NORSAR (Norwegian Seismic Array) was the first international node and established the connection further to the next node at University College London, UK, see http://www.fulbrightalumni.no/andr-rnes/

[7] See http://en.wikipedia.org/wiki/Mosaic_(web_browser)

[8] The University of Illinois, United States.

[9] See http://en.wikipedia.org/wiki/Netscape_Navigator

[10] See Justice Stevens opinion of the Court in United States Supreme Court Case No. 96-511, June 26, 1997, Page 18.

2. THE HISTORY OF COMPUTER CRIME AND CYBERCRIME BEFORE 2000

Computers were introduced to the global societies in the early 1950ties. In the beginning the computers complexity limited their availability, but by and large they become less expensive in addition to a continuously improved reliability and capacity. Especially a dramatic technological evolution occurred, creating the big mainframe computers and minicomputers.

The Society for Worldwide International Funds Transfers (SWIFT) was introduced to the international banking systems in 1978 and was immediately regarded as the most secure commercial global computer networks.

As computers developed, so did also crimes assosiated with their use. Mankind will always have to live with criminal activity, and as a result of the conversion to computer usage, new methods of perpetrating crime occurred. The term computer crime or computer-related crime was used as a description of this new phenomenon.

Computer crime became also a subject for researchers, as well as investigative efforts for law enforcement and legislative initiatives. In a Hearing before the US Senate in 1978, the FBI testified that they had conducted investigation in approximately 50 cases, mostly alteration of computer data input, theft of computer services, theft of data and alteration of data, as computer programs for either financial gain or destructive intent. But most computer crimes were investigated and prosecuted at the State level.

As with other technology development in the 1970ties, the development of computer technology was evaluated with

regard to penal legislation. The existing provisions in the Criminal Codes were not written with computers in mind, and the main challenge was the applicability of these provisions on automated data processing and to what extent. The processing and storing of data by means of electronic impulses represented invisible and intangible values for governments, private industry, and individuals that clearly should be protected by criminal law. If the existing provisions in the Penal Codes were insufficient, it was decided that new solutions should be developed.

It was also emphasized that this problem must be solved in view of the international application of automatic data processing.

Even from the early years on a large amount of detected cases were not reported. Victims, such as governmental institutions, private industry, and individuals were reluctant to report computer crimes, fearing bad publicity, or loss of confidence, or more criminal attacks.

2.1 The Pioneers

The founder and father of the knowledge of computer crime, is by many observers considered to be Donn B. Parker, USA.

Donn B. Parker was involved in the most exhaustive research of computer crime and security from the early 1970ties.[11] The research compiled by the end of 1970ties more than 1000 reported cases from around the world. He served as a Senior Computer Security Consultant at the SRI International (Stanford Research Institute), Menlo Park, California, and was the main author of the first basic federal manual for law enforcement in USA: “Computer Crime – Criminal Justice Resource Manual on Computer Crime” (1979).[12]

This Manual soon became an encyclopedia also for law enforcement outside USA.

Attorney Susan Hubell Nycum was working together with Donn B. Parker on projects and provided a paper on legal issues relating to computer abuses for the US Senate Committee on Government Operations in the Committees study of Computer Security in Federal Programs (1976-77). Susan Nycum published also an article for the American Bar Association Journal on the legal issues for computer crime in 1975.

Another researcher was Edward H. Coughran. He was the Director of the Computer Center, University of California, San Diego, and organized at the university a Symposium on Computer Abuse for Prosecuting Attorneys in 1976.[13] He developed the Symposium with the stimulation and cooperation of the US Attorney in San Diego.

Professor Brandt Allen, Colgate Darden Graduate School of Business Administration, University of Virginia, presented a paper on “The Computer Thief” at a Seminar in 1974.[14] He presented also a paper on “Embezzler ´s guide to the computer” in Harvard Business Review (July-August 1975).

Other authors in USA that contributed in the combat against computer crime in the early days were August Bequai[15], Jay J. Becker (BloomBecker)[16], and Thomas Whiteside.[17]

Ulrich Sieber, University of Freiburg, Germany, became the first academician expert on computer crime outside USA in the 1970ties.[18] He assisted many international organizations, such as the OECD from 1983 and United Nations.

In Australia, Justice M.D. Kirby, Chairman of the Australian Law Reform Commission, was leading the development and emphasized “*computer crime and the need for new laws*

and procedures to deal with anti-social conduct involving misuse of information technology."[19]

K. E. Brown, a detective chief inspector at the Victoria police in Melbourne was also early involved in the combat against computer crime.[20]

In the Netherlands, H. W. K. Kaspersen, also an academician, was in 1986[21] an expert on computer crime, and became later the "father" of the Council of Europe Convention on cybercrime, through his initiative in 1997.

In Canada, Donald K. Piragoff was the leading expert, and published an article in 1986 on *Combatting Computer Crime with Criminal Laws.*[22]

In Norway, Stein Schjolberg began to work on computer crime from 1976 when he was introduced to computer crime by FBI. He then introduced INTERPOL to computer crime in 1979 and organized a global seminar together with INTERPOL in 1981.

2.2 The Pioneer Bill – The Ribicoff Bill, United States Senate

The United States General Accounting Office (GAO) issued in April and May 1976 three reports on problems associated with computer technology in Federal programs. [23]

The first report of April 23, 1976, was entitled *"Improvements Needed in Managing Automated Decision-making By Computers Throughout The Federal Government."*

The second report also of April 23, 1976, was titled *"Computer-Related Crimes in Federal Programs".*

The third report of May 10, 1976, was titled *"Managers Need to Provide Better Protection For Federal Automatic Data Processing."*

The reports were delivered to Senator Abe Ribicoff, as the Chairman of the Senate Government Operations Committee. Senator Ribicoff announced on May 10, 1976, that the Committee staff would begin a preliminary investigation concerning issues raised in the GAO reports. On June 21, 1976, the Senate Government Operations Committee published a 447-page committee print containing the three reports, entitled *"Problems Associated with Computer Technology In Federal Programs and Private Industry."*

A staff study of *Computer Security in Federal Programs* by the U.S. Senate Government Operations Committee was then published in February 1977, and this study was the world's first comprehensive initiative on computer crime. The staff study addressed several problems associated with computer programs and obtained information on computer security practices and problems from several individuals and federal agencies.

Attorney August Bequai provided information on the role of the computer in white-collar crime.[24]

Attorney Susan Hubell Nycum presented a paper on the legal aspects of computer abuse based on a project at the Stanford Research Institute (SRI), Menlo Park, California.[25] The SRI project was headed by Donn B. Parker and had identified 420 cases of computer abuse.

The Staff of the Senate Government Operations Committee made a conclusion and proposals on the legislative issues as follows:[26]

> *There is ample evidence to suggest that much of the computer-related criminal activity has involved, or will involve in the future, government computer systems.*