The History of Information Security: A Comprehensive Handbook
Karl de Leeuw and Jan Bergstra (Editors)
© Published by Elsevier B.V.

1

INTRODUCTION

Karl de Leeuw

Informatics Institute, University of Amsterdam
Amsterdam, The Netherlands

Contents

Abstract

This introduction gives an overview of the topics dealt with in this Handbook, and reaches the conclusion that society at large has to come depend increasingly on a civilian deployment of security tools. This unprecedented dependence entails risks of its own which are insufficiently weighted in current accounts of the impact of the digital revolution.

Keywords: communication security, identity management, intellectual ownership, cryptography, computer security, privacy, information warfare.

1.1 AN EXAMPLE FROM DUTCH HISTORY

The history of information security does not begin with the advance of the telegraph, the wireless, or the Internet. This claim is amply illustrated by an anecdote from Dutch history.

In January 1684 the Dutch Republic and France were on the brink of war. The French had attacked the Southern Netherlands which at that time was still a part of the Spanish Empire, and it seemed unlikely that the French would halt should the Spanish have been defeated. They had tried to conquer Holland twelve years before and there was little reason to trust their declarations of good will. Therefore, Stadholder William III, a semi-hereditary commander of the army and navy as well as chief executive of the foreign policy of the Republic was willing to fight the French in the Southern Netherlands.

The French ambassador in the Dutch Republic, Count D'Avaux, had no inclination to wait until William had succeeded. He entered direct negotiations with the city council of Amsterdam in order to prevent that city from raising money for troops as the stadholder had requested. Count D'Avaux's negotiations could easily be construed as a direct interference in the internal affairs of the Dutch State, but it was not uncommon for a French ambassador to do a thing like that. The stadholder, however, wanted to make a point of the counts activities and had the ambassador's messenger shadowed at a time when he was most likely carrying a letter on the negotiations to the King.

The courier was captured just after he crossed the border near Maastricht, by horsemen clearly belonging to the Maastricht garrison. The courier, robbed of all of his belongings except for his boots and his jacket, returned to his master with the story of what happened. The affair caused much distress to the members of the Amsterdam town council, but D'Avaux reassured them that the letter was fully coded and that no one could read it without a key. On 16 February 1684, however, the stadholder entered a meeting of the Amsterdam city council with a decoded copy of the letter, accusing its senior members, Hooft and Hop, of treason.

William claimed that he had received the copy from the governor of the Spanish Netherlands, De Grana, which made D'Avaux laugh. The only thing D'Avaux still could do to help his friends at the town council was to pretend that William's cryptanalyst had interpreted the letter wrongly and to support his claim be provided a 'genuine' copy for circulation. In turn then, William III released a copy, at first leaving out many of the unsolved code groups. Somewhat later, he released a full version in plain text, accompanied by the solutions from other letters which were also intercepted at the same time and which were even more compromising (Kurz [18]).

This incident made William III, who was to ascend to the British throne in 1689, well aware of the benefits of intercepting mail. In this case, he had used the information immediately and without effort to hide its source in order to provoke a crisis. As King of Britain, a few years later, he would commence with intercepting mail on a regular basis for purpose of strategy planning. Thus a trend began: during the 18th century, most countries employed code-breakers, linguists, and clerks to intercept the mail of foreign diplomats on a regular basis.

This example serves to illustrate the core concepts of information security. The ambassador's courier, travelling back and forth to the Court in Versailles, was a component of the French diplomatic information system which assured that the French emissaries abroad would keep the King informed in order to carry out his will. The loyalty of the courier, often a personal servant of the ambassador, was of vital importance for the system, as was his good health and general fitness of the horse. The encryption of the letters he carried, acted as a second line of defence. Thus, for this example, the protection of communication security depended upon three components: psychology, physical integrity, and encryption. A fourth element that is, diplomatic immunity provided the legal context for the French information system. It was significant that the robbing of the courier did not take place in Holland but rather just across the border. The Spanish were already at war in the Southern Netherlands; whereas the Dutch were not. Consequently exposing French interference in the internal affairs of Amsterdam as well as the treason attempt by members of the town's council was an excellent instrument employed in removing political opposition and turning public opinion against the French. It is information warfare at its best.

1.2 DEFINITIONS, TOPICS, AIM

This story from the 17th century remains a surprisingly relevant one for a proper understanding of the core concepts of today's information security, which is usually defined as: "the protection of information and information systems against unauthorised access or modification of information, whether in storage, processing, or transit, and against denial of service to authorised users. Information security includes those measures necessary to detect, document, and counter such threats" (Jones, Kovacich and Luzwick [16]).

Information system security, deals with "the entire infra-structure, organisation, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information". This definition is independent of any stage of technological development, which means that it can be applied both to the courier services of the early modern world and to computer networks of today.

A similar approach is taken by Bruce Schneier in *Beyond Fear* [26, 6]. He argues that security concepts apply, or should apply, equally to computers and to the world at large. He defines a security system as a "set of things put in place, or done, to prevent adverse consequences. It is concerned with intentional actions which are unwarranted from the point of view of the defender, not necessarily illegal" [26, 12]. A security system presupposes a security policy requiring someone who defines it which generally is the asset owner [26, 34–36]. Those security policies reflect the political agenda of the owner(s) or a trade-off among various interested parties who move power in varying degrees from one set of players to another and who are anything but value-neutral. Taken in this manner, information security consists of the entire range of instruments available to limit the flow of information, including those theories, practises and insights that allow us to put them to good use. In a sense, we are dealing with an armoury for the exercise of social control [14].

Of course in information security, political and ethical considerations are particularly relevant. Information security consists of the entire range of constraints deliberately built into any information system in order to restrict its use. These constraints may encompass legal measures, institutional frame-works, social practises, or instruments, including devices or machines developed especially for that purpose.[1] These constraints are expressions of the wishes and perspectives of the system owners. Thus, the history of security technologies may well serve to illustrate MacKenzie's and Wajcman's thesis that the actual shape new technologies take on reflects the interests of the parties involved in the design process [22].

The aim of this book is to gather materials from different disciplines for a reconnaissance tour of the security domain of information systems. It is intended first as a field-survey and consists of twenty-nine contributions, dealing with episodes, organisations, and technical developments which are, in one way or another, exemplary or which have played an important role in the development of information security. The chapters are written by experts in such diverse fields as computer science, law, history, and political science and are arranged into six sections. The sections on computer security, and on cryptology and communication security, constitute the core of the book and stay firmly within the traditional scope of information security. The section about intellectual ownership may surprise some readers. However, its inclusion is justified by the fact that copyright and patent registration systems are important instruments to define intellectual ownership while also providing organisational and legal means of enforcement.

Moreover, it provides a background for the debate about the propriety of software. The main argument in favour of Open Source software is that without it no software transparency, and therefore no computer security, can ever exist. The chapters in this section show how the Open Source movement borrowed key concepts from scientific publishing and also that alternatives do exist in the form of protecting software through patents or copyright. The section about identity-management includes chapters about biometrics, the collection of data about state subjects, and security printing. It aims at a better understanding of this topic through a multi-faceted approach. The fifth section deals with privacy and export regulations. These regulations are particularly relevant for the way information security is practised and have constituted hotly debated political issues in both Europe and the US. The sixth section contains only one contribution about information warfare. This part explores the strategic meaning of information security and addresses the question whether the information society of today encounters unprecedented threats.

Three questions will recur throughout the book. How did political or ethical motives influence the choice or shape of security instruments? Did scientific research, or new technological developments, influence legal practises or the execution of certain policies? Did technological or scientific considerations ever act as constraints for the formulation of political ambitions? In which ways can the availability or lack of security instruments be seen to act as a strategic consideration in the political debate?

1.3 HISTORIOGRAPHY

The origin of information security can be traced back to the rise of hierarchical command and

[1] There is some debate about the question whether the legal frame-work should be considered part of the security system. I like to follow Donn Parker [24, 36] who says it does.

control structures in administration and warfare from civilisations of the ancient world. Plenty is known about administrative procedures or command structures in western history, but there has been little effort to highlight the elements of confidentiality, integrity, and availability that figure so prominently in contemporary literature about information security.[2] Unfortunately, the extensive literature dealing with the rise of the Information Society does not pay any attention to security issues either (Toffler [28]; Beniger [7]; Agar [1]; Bijker, Hughes and Pinch [8]; Machlup [21]).

There are, however, very substantial contributions to the history of sub-areas. The history of cryptology has enjoyed considerable attention, for instance, particularly after Kahn published his epoch-making *Codebreakers* in 1967 [17]. The focus of the research since then is mainly on code-breaking and signals intelligence during World War II which was dominated by Anglo-American perspectives although Cold War research has also gained importance in recent years (Aid and Wiebes [2]). Moreover, military historians have paid considerable attention to command and control structures.[3] Contemporary cryptology is largely uncovered, with the exceptions of Simon Singh's *Codebook* [27] and Stephen Levy's *Crypto* [19].

The history of computer security has not been a topic for research thus far but, to a certain extent, hackers and free software have been researched.[4] There is a vast literature about the history of patents, and to a lesser degree, about the history of scientific publishing and copyright. The history of identity-management as such has never been investigated, but parts of it have been, such as the issuing of passports (Caplan and Thorpey [11]) and the use of biometrics (Breckenridge [10]), albeit in a forensic context mostly (Beavin [4]). Some case studies have also been written, and Edwin Black's controversial and disquieting *IBM and the Holocaust* [8] may serve as an example. The privacy debate is closely related to identity-management issues, but has not resulted in historical research of any substance. The contributions of Bell [5;6] and Westin [29], do show a strong concern for the societal implications of the application of new information technologies, which may prove of heuristic value. Needless to say, this list is far from complete. I refer to the contributions in this book for further reading.

1.4 LIMITATIONS

This book may be a little disappointing for those wanting to know more about industrial espionage or more generally about information security in the context of corporate business, and this author is well aware that most practitioners today are keenly interested in protecting company assets. The focus of information on security in the corporate world, consequently, would be on assuring the continuity of business processes, industrial espionage, or the disruption of communication structures with criminal intent; these subjects certainly are part of a much larger portfolio. Unfortunately, this author has not been able to locate writers for this important subject. It should be noted, however, that safety, or the protection of assets from unintentional hazards, is not a proper part of this book since its intent is to cover security issues intentionally inflicted.[5]

A similar remark must be made for those wanting to know more about information security in the context of bureaucracy. The concern for confidentiality, integrity and availability of information has been an integral part of administrative practises for centuries. Unfortunately, in as much as the history of administrative practises has been written, there has been no effort to link it with the history of information system security.[6]

[2] For an introduction see for instance Gollmann [15] or Anderson [3].

[3] See for instance: John Ferris, *Airbandit C31 and strategic air defence during the first battle of Britain, 1915–1918* [13].

[4] See for instance: Steven Levy, *Hackers* [20]; Eric S. Raymond, *The Cathedral and the Bazaar* [25]; Sam Williams, *Free as in Freedom* [30].

[5] For the difference between safety and security see Schneier [26, 12].

[6] Angelika Menne-Haritz [23] has written extensively about the development of administrative procedures in Germany, but she did not provide a link with security.

This book then focuses on western history since the Renaissance. The basic ideas about intellectual ownership and the accessibility of knowledge were all formed during the 16th century in the western hemisphere as were core concepts in administrative organisation and diplomacy. This emphasis does not mean that the history of the empires of the ancient world, or the history of the great empires of the eastern hemisphere, will not provide interesting parallels, but these subjects necessarily fall outside the scope of this book.

1.5 INTELLECTUAL OWNERSHIP

In the first contribution examined, Jack Meadows has taken a close look at the way scientific publishing has evolved in early modern Europe. Before the 16th century, the idea of scientific publishing was virtually unknown. Scientific research took place in the context of alchemy or of secret societies, given to theosophical speculation, and scholars tended to adhere to secrecy if only to avoid being burned at the stake by the Papal Inquisition. The publication of Copernicus' *De Revolutiones Orbium Coelestium* by a protestant scholar, defying the authority of the Roman Catholic church in 1543; the publication of *De Humani Corporis Fabrica* by Vesalius in the same year; and two years later Cardano's *Ars Magna* in 1545 all marked a sudden change in scientific publishing. Part of the reason for the bold change was that the printing and distribution of complex texts and drawings had become easier. The fact that the career perspectives of scientists and scholars became increasingly dependent on personal fame also mattered. Thus Vesalius owed his appointment as personal physician of the Emperor Charles V directly to the publication of his book.

During the 17th century the cumulative structure of scientific knowledge became widely acknowledged and along with it a principle of scientific priority. The need for secrecy did not vanish, however; but it did become tied to the need of conducting verifiable experiments to support theories. Initially, priority claims were safeguarded by hiding a short reference to a discovery in an anagram and putting this at the disposal of a well-known colleague. Later, the depositing of a sealed and dated manuscript at a scientific academy came into vogue which had the advantage that much more detailed claims could be substantiated. During the 19th century, this depository practise vanished because by then it was commonly believed that the priority should go to whoever first published a discovery not to whomever the thought first occurred.

The 19th century, with its quest for scientific progress, marked the heyday of the scientific journal, and this pattern of scientific publishing is still with us today. The point of departure today is that the progress of science is best served by the free exchange of ideas even though this concept is not taken too literally. Scientific journals themselves act as a bottleneck since each is free to accept or reject the publication of a scientific paper. An initial rejection by one journal and a subsequent acceptance by another may result in a delay of years. The system of peer review used by most journals to rule out idiosyncrasies of the editing staff can turn counterproductive when a referee wants to avoid publication of anything threatening his authority.

Moreover, political pressures may also still be operating within this system of scientific publication. The arrest and trial of Galileo in 1632 is probably the best known example, but in the totalitarian regimes of the 20th century similar events have happened. For example, the purging of Jewish elements in physics by the Nazis which led to a discrediting of quantum physics and relativity theory is one example, and the ban on the publication of research based on Mendelian principles in Soviet Russia is another since traditional genetics did not fit communist beliefs. The western world is not exempt from restraints either. The classified research on behalf of the defence industry or contract research for commercial purposes may easily clash with the scientists' needs to make advancements known. The electronic publication of preprints has added to the armoury of the scientific author, but this solution does not remove any of the restrictions already mentioned. Scientific publishers may demand removal of the preprint from the Internet as soon as it is published in a magazine in order to make sure that revenues are not lost.

In the second contribution, Kees Gispen deals with the history of patent law with particular reference to the German patent system in the early 20th century. The first patents were granted the in late 15th century in Venice and in the early 17th century in England to 'men of exceptional genius' or 'first and true inventors' for accomplishments which would greatly benefit the 'common good'. These patents were privileges, however, not rights so there was no concept of intellectual property at stake either since the primary motive of the accomplishment was to benefit the common good of a state.

The concept of intellectual property itself waited until John Locke's 'natural right of proprietorship' was written. This concept lay at the root of the patent system which was introduced during the French Revolution in 1791, but it also affected practises in Britain where the concept of 'societal utility' acted as a counterbalance. By the end of the 18th century, both France and England were ready to dispose of state-granted monopolies used in the past. It was not self-evident, however, that patents and free trade could go together. Scottish philosophers, such as Adam Smith, believed they could, but exponents of the Manchester School later believed patents and free trade did not go well together.

The Manchester School sparked off an anti-patent movement with considerable influence in The Netherlands, Switzerland and Germany which lasted until the last quarter of the 19th century. The United States remained unaffected, however, since the concept of 'natural propriety rights' is firmly rooted in the US constitution. Following the French example, the United States adopted a patent regime based on the 'first-to-invent-principle', or to put it differently, based on the 'authorial principle'. In this way, an inventor's rights were well protected even though this system worked only when an innovation occurred within the context of small-scale enterprises.

By the end of the 19th century, the inventor-entrepreneur was no longer leading the way. By then, most innovation took place in the context of corporate businesses by employees more often than not working as a team. The basic ideas behind the US patent system were not abandoned, however; but the US law did allow employers to claim the ownership of the inventions of their employees through an explicit clause in the employment contract. In reality this approach meant that inventors had little control over their inventions, but they did retain the non-material claim to the invention and were free to change employers or to start their own businesses.

Germany took a different course. After its unification in 1871, the Second German Empire was confronted with a bewildering diversity of patent regimes in the various states as well as an abolitionist movement inspired by the Manchester School. The leader of the pro-patent movement was Werner Siemens, a brilliant inventor-entrepreneur and head of the Siemens electrical company. He argued that German industry could not do without the legal protection of its inventions. The patent system should defend the interests of the industry not the interests of the inventors who were unable to act without the support of industry. With his influence, then, Germany adopted the first-to-file principle, meaning that whoever filed a patent first legally owned it. The German patent system allowed companies to claim that the inventions were made collectively, and therefore, the intellectual property of the company which, quite naturally, caused resentment among German engineers and which, in turn, resulted in political strife which was finally settled in 1957. Gispen argues, then, that the German system did not encourage inventors to start their own businesses as happened in the United States. Rather German patent laws encouraged conservative inventions within the context of existing large research establishments which, in the long term, was detrimental to innovation.

In the third contribution, Chris Schriks and Rob Verhoogt explore the emerging copyright protection in particular reference to The Netherlands. During the early modern period, The Netherlands had been the preeminent publishing house of Europe because of an absence of censorship and because of the presence of highly skilled immigrant communities who were on the run for religious and political oppression elsewhere. In countries like England and France, copyright protection had been part of the exercise of state and religious censorship, but in the Dutch Republic copyright protection was granted by way of privileges by requests of printers' guilds where the motive was purely economical, that is to say to protect the interests of an important industry.

The concept of intellectual ownership was introduced during the French occupation of The Netherlands under the influence of Enlightenment thinking and actions taken abroad by authors such as Pope, artists such as Hogarth, and composers such as Verdi. This period marked the beginning of the emancipation of the author from a publisher. The idea that the copy needed protection but the original work did not remained present not only in The Netherlands but also elsewhere. This preference of copy protection over original work protection can be seen when copyright protection was extended to images, meaning that engravings were protected yet the original images were not. This preference for copy protection resulted in heated debates which lasted for almost a century between authors, artists and composers on the one side and vested economic interests on the other. As late as 1877, the Dutch jurist H. Viotta argued, as a matter of principle, that copyright protection related exclusively to the multiplication of material objects and not to the spread of ideas.

The invention of new reproduction techniques, such as photography, sound recording, and in their wake film made a redefinition inevitable. The Berne Convention of 1886, and its revisions of 1908 and of 1928, gave due weight to the role of creative genius, and more or less enforced conformity of copyright regimes between western countries allowing for national differences to fade. The rise of the new distribution media which reached into people's homes through radio, television, tape recorders, and even copying machines could be used for limited scale multiplication made a revision of copyright rules necessary. The concepts of publishing and multiplying diverged, and the difference between private and public use was no longer always easy to make. The Internet, and the accompanying concept of Digital Rights Management, marks a new stage in the development of copyrights through the centuries which includes the idea that technological changes might force changes in legal areas which does not necessarily mean that guiding principles of the past have become obsolete. The emergence of concepts such as Creative Commons or Free Source, which focuses on the idea of freely publishing technical information for every one to use and with no profit intended, may be taken a step further in the emancipation of the author from a publisher.

In the fourth and fifth contributions, Madeleine de Cock Buning writes about copyright protection for software and Robert Plotkin writes about the protection of software through patent law. Both subjects may traditionally not have been counted as security-related topics but in reality they very much are so related since they exemplify alternative ways of protecting the ownership of software without making source code unavailable for research purposes. An extension of patent and copyright law regimes to software may reconcile the interests of proprietary software developers and the need for code inspection in the name of public welfare. De Cock Buning explores the experiences with copyright law made after the 'unbundling' of soft- and hardware by IBM in 1970. The first efforts to extend a copyright regime to the protection of software were made shortly thereafter and proved less straightforward than one might think since both the algorithm and the actual expression in programming language need protection and copyright law traditionally only addressed the latter issue.

The tendency, then, both in Europe and in the United States has been to develop a new protection regime. In the US this resulted in a demand for a proof of arbitrariness of computer programs to ensure that the algorithm was not protected as well. In Germany, legislation required an 'exceptional originality' to justify the invocation of copyright protection. Needless to say neither solution has proven to be fully satisfactory.

Robert Plotkin explores the history of software patents by reference to a number of particular controversial cases in the US and to actual and proposed legal reforms in the US and Europe. He concludes that the ambiguous nature of software, described only in abstract or logical terms but always designed for a specific application, has made it difficult for patent law to formulate suitable criteria for patentability.

Jurisprudence has succeeded in fleshing out arguments in such a way that patent lawyers now know with reasonable certainty which requests are likely to be granted. Legislation has not, however, been able to resolve the root problems represented by the tensions between competing legal rules. Plotkin signals the rise of new problems due to the granting of patents for automated design processes; this new difficulty makes the line between 'idea' and 'application' even more difficult to delineate. Moreover, the granting of patents for fully automated business processes has torn the wall between industry and the liberal arts which will make the enactment of new legislation inevitable, even though policy makers are reluctant to take up the responsibility for this new legislation. This situation is slightly better in Europe than in the US as the aborted European Software Directive indicates.

1.6 IDENTITY MANAGEMENT

The second part of this book deals with identity management. The modern state cannot exist without knowing who its citizens are, and neither can banks exist without knowing who its customers are. The registration of ownership of land, houses, and movable properties is a prerequisite for both economic transactions and tax levying. Pieter Wisse develops a semiotics of identity management in three parts. In the first part (Identifying assumptions) he introduces how pervasive issues of identity really are. Philosophy, science and, not to be neglected, religion may indeed be viewed as attempts that come to terms with identity where ownership is concerned. In the second part (Identity in enneadic dynamics) Wisse presents an encompassing framework, inspired by C.S. Peirce, which is an enneadic model of semiosis which in turn is then applied to a pragmatic design, or a behavioural, orientation for identity management.

Communication and identity management are largely synonymous; identity management is essentially dialogical. Illustrations from natural history serve to emphasise the generally valid behavioural orientation. In part 3 (Social practises in identity management) Wisse illustrates how the semiotic framework helps to provide an overview of perspectives and discusses selected developments in identity management at the cultural level, that is as practised by human communities and societies. The partly electronic future of identity management is proposed as a program for open security in an open society.

Karel Schell treats the subject of document security, and more notably the security of banknotes, from their introduction in the 17th century until now. The history of banknotes provides us with a classical example of identity management. The banknote was introduced at various times and by various agents in order to facilitate money circulation, but it only proved successful after the emergence of a reliable system of central banks able to conduct a sound monetary policy. This system finally took shape around the year 1800 after two centuries of rigorous efforts, many of which went wrong.

The development of security printing was dependent on the existence of an authority willing to vouch for the authenticity of the document at hand which also meant that the document had to contain features that made reproduction difficult. Initially this purpose was served by the application substrate marks such as watermarks and security threads, or the use of unique type fonts, for instance the type fonts for the printing of music, invented by Johan Enschedé around 1780. The invention of photography around 1840 added new features to the armoury such as colour and eventually guilloche printing. Guilloche printing consists of complicated, engraved line patterns that are impossible to reproduce because of the subtle variety in distances between the lines.

The introduction of offset printing and colour scanners between 1920 and 1950 made the development of new deterrents necessary. The vulnerability of existing practises is exemplified by a number of cases of successful counterfeiting between and during the world wars which were mostly, but not always, politically motivated. The counterfeiting of British Pound notes by the SS is the most famous example. The deliberate introduction of moiré patterns, occurring when two periodic patterns, such as an array of straight lines or a series of concentric circles, are overlapped with imperfect alignment which would become visible when reproduced proved to be a helpful answer.

The invention of the laser colour copier and the digital revolution during the 1980s added optically variable printed images, holograms and covert images to the armoury. Interestingly, some substrate-based security features, such as watermarks and security threads, present for the last two centuries, proved far less vulnerable; whereas, the numbering of banknotes continued to be an indispensable means of identification. Moreover, the general requirements for banknotes have always remained roughly the same and were already listed in a report written by Sir William Congreve for the British Government in 1819. His point of departure was that security features should be "immediately recognised and understood by the most unlearned persons".

The use of micro text, incorporation of the serial number in the watermark, and guilloche structures were advocated by him as deterrents against counterfeit decades if not a century or so before their actual applications. The history of banknotes provides valuable clues about the history of identity management in general. Firstly, the need for 'virtualisation' is older than the digital age hence precedents can be found in the quest for security technologies. Secondly, the state of technology limits both possibilities and threats, which also means that technological progress does not allow more than temporary preponderance. Thirdly, general principles or guidelines can be established that may outlive a particular state of technology provided that the goals are sufficiently clear.

Edward Higgs depicts the development of identification techniques and indeed the various transformations in the concept of identity in England from the late middle ages onwards. England is a particularly interesting example since at various points in its history it played a leading role in the introduction of new identification techniques, such as a system for fingerprinting in 1901 and DNA-profiling in the 1980s. Higgs discerns three broad stages. During the early modern period, identification took place within the community in which a person lived or by lineage. During this period, the state was not the centralised, almost omnipotent entity it is today but rather a sphere of governance. The state formed a national community of those in every locality who were willing and able to be involved in the exercise of authority. For the lower strata of a society this framework meant that identification was a local matter. For the aristocracy and gentry, identification was bound up with proving descent through genealogies and involved the use of antiquarians to prove that one had the right to a name, a title, or land.

Characteristically, the Poor Laws of the 16th and 17th centuries intended to encourage and rationalise charity focused entirely on proving that the poor really belonged to a parish. Therefore, wandering beggars or vagabonds were flogged in public, put in jail, and finally physically branded. During the 19th century, urbanisation and industrialisation came with other more centralised forms of control. Local communal forms of governance proved unable to cope with the creation of vast, urban conglomerations while local elites ceased to be interested in the locality as their wealth increasingly came from positions or shares in national or international companies.

The individual increasingly had come to be captured in a nexus of centralised state registrations which identified him as a property-holding citizen. At the same time, those who did not take part in civil society had to be put under surveillance. The New Poor Law of 1834 ruled that the poor had to submit to imprisonment in all but name in so-called workhouses. Various criminal registries were set up, at first with limited success and from 1871 onwards improvements were made with the introduction of photography, body measurements, and fingerprinting. The increasing speed of transport added to pressures for more national forms of identification. Typically, the first sign was the introduction of the driving licence in 1903. Finally in 1915, the first modern UK passport was introduced with a description, a photograph, and a signature. In itself this identification use marked the beginning of the third stage in which bodily forms of identification were extended to the citizen instead of being reserved for the alien and anti-social elements in society.

The growth of the welfare state, beginning with the National Insurance Act in 1911, and the increasing role of banks and other financial institutions made some form permanent identification necessary. Efforts to introduce a British identity card, however, met with much resistance, except in war time, particularly from the conservative strata of society. The resistance continued well into the 1970s until it became clear that welfare benefits were often unjustly claimed. The government, then, tried to curb the abuse by verifying and cross-checking personal data in computerised databases. To that end the national insurance number was introduced. In 1989, 1994 and 1997, debates about a national registration and national identity cards surfaced without any tangible results. In 2004 the labour government tried to solve this issue once and for all by submitting its Identity Card Bill to Parliament. This bill called for the introduction of a national identity card with various biometric features including DNA-sequences so that this card was intended to be processed by machines.

Jim Wayman focuses on the rise of automatic recognition systems since the 1960s. He defines biometrics as "the automatic recognition of living individuals based on biological and behavioural traits". This idea is a clear departure from the traditional definition, which includes the fingerprinting, photographing, and measuring techniques done by hand as developed around 1900 by people like Galton and Bertillon. Wayman shows that during the 1960s, expectations were high. In 1963 Michael Trauring wrote that, biometrics in this sense of the word promised, "personal identity verification in seconds, requiring almost no trained or skilled operating personnel, with the advantage of not being susceptible to forgery or theft".

Technological developments for these processes fell far behind however. Early experiments with fingerprinting proved that they could easily be forged; whereas, facial recognition still lacked a sound technological basis to be of any use. Speaker recognition and automatic signature recognition performed slightly better, but computer technology was still insufficiently advanced to allow for any large scale applications. In 1970 biometrics moved more to the foreground, due to the start of a formal testing of fingerprint systems by the US National Bureau of Standards and included, in particular, holographic optical techniques for forensic purposes. In 1971, the US National Academy of Science organised a working group on speaker verification and the Acoustical Society of America held a meeting devoted to spoofing speaker recognition systems through mimicking.

In 1974, both the Stanford Research Institute and the National Physical Laboratory in the UK began working on signature recognition systems, and hand geometry verification was actually put to practise by the University of Georgia. In the same year, the US air force announced a program for a military-wide biometric identification system for access control that used a combination of biometric features to reduce error rates. The system was intended for production in 1980, but it was never deployed on the hoped for world-wide scale. In 1975 the Mitre Corporation followed with a formal test program for fingerprint, voice and signature recognition, and in 1977 the National Bureau of Standards (NBS) published a Federal Information Processing Standard for Automatic Personal Identification (API).

The twelve criteria for device evaluation, listed in this document are still applicable today. In 1983, formal testing programs were launched by the US Department of Energy and the US Department of Defense. The decision by California, to require fingerprints for driving licences met with resistance from congress so that this example was not followed by other states. Generally speaking, government agencies showed a greater interest in biometrics both in development and application than did businesses. This tendency continued during the 1990s. In 1994, a National Biometric Test Centre (NBTC) was launched by the Biometric Consortium, under joint control of NBS and National Security Agency (NSA). At approximately the same time, the European Commission founded the BIOTEST program at the UK National Physics Laboratory.

During the last decade of the 20th century sales of biometric devices increased a hundred fold whereas revenues increased ten fold. The actual application of biometrics systems remained limited, however, and was, or is, still largely experimental in nature. During the first years of the 21st century, pilot projects for frequent air travellers have been, and still are, undertaken in The Netherlands, the UK, the US, Germany, Malaysia, and Australia. The results seem to indicate notwithstanding the technological progress that has been made over the years that biometrics is still insufficiently reliable to be implemented on a large scale. In that sense, the call for application of biometric features on national identity cards by the US congress, with other countries voluntarily or involuntarily following suit, seems premature.

1.7 CRYPTOLOGY AND COMMUNICATION SECURITY

The third part of the book deals with cryptology and communication security. Gerhard Strasser depicts the development of cryptology in Europe during the Renaissance and thereafter. Cryptology was already being practised by the Greeks and the Romans during ancient times, but there is little proof of anything beyond mono-alphabetic substitution ciphers, let alone any form of cryptanalysis. During the middle ages most of what the ancients did or knew appears to have been forgotten, but Jewish mysticism encouraged an interest in the hidden meaning of biblical texts through assigning number values to letters and words. Jewish scholars engaged in such speculation had no interest in improving communication security, but their work became a source of inspiration for leading cryptologists during the Renaissance, such as Trithemius and Vigénère.

The first Treatise on cryptanalysis, however, was written during the 9th century by the Christian Arab philosopher Al Kindi. Unfortunately, his contribution remained largely unknown in the west, notwithstanding the inclusion of a vast amount of cryptological knowledge in an encyclopedia of Islamic knowledge by Ibn Ad-Durayhim in 1412. The real origin of cryptological thinking in the west lay with the rise of the Italian city states during the 14th century and the invention of standing diplomacy. As a result, diplomatic dispatches had to be ciphered on a daily basis which gave rise to the emergence of a new type of official: the cipher clerk or cipher secretary. People like Argenti in Rome, Soro in Venice, and Simonetta in Milan wrote their treatises on cryptanalysis in secrecy for the dual purpose of improving the ciphers and codes of their masters and the training of new colleagues or successors.

During the 15th and 16th centuries, many cryptographic inventions were published by scholars such as Alberti, Bellaso, Porta and Cardano. Virtually all important cryptographic principles and devices were described in their books, ranging from the cipher disk and cipher square to the autokey and super enciphered codes. In 1624 this whole body of knowledge was comprehensively summarised by August Duke of Brunswick-Wolfenbuttel, writing under the pseudonym Gustavus Selenus. His book, *Cryptomeytices et Cryptographiae Libri IX*, became the standard reference work for the next two hundred years. The late 16th and early 17th centuries, an age of civil and religious warfare, saw a gradual proliferation of cryptological knowledge throughout the rest of Europe, with outstanding contributions in the field of cryptanalysis by mathematicians such as Viete in France, Wallis in England and Rossignol in France.

After 1650 the focus of many authors shifted to the search for universal language schemes, usually to facilitate the conversion of exotic peoples to Catholicism. Jesuit scholars such as Athanasius Kircher, Pedro Bermudo, or Kaspar Schott practised cryptography more or less as a side show of their ambition to spread Christianity through scholarly means which does not mean that their schemes and systems lacked practical value. Kircher, for example, invented a kind of cipher slide, the so-called *Arca Steganographica*, which proved a rather useful encryption tool for many courts in Europe. Generally, the popularity of universal language schemes in literature does not tell much about prevailing cryptological practises.

After the Peace of Westphalia in 1648, a system of standing diplomacy was adopted in all of Europe and was similar to the system that had existed in Italy before. This adaptation stimulated the diplomatic use of cryptography and lead to the emergence of a class of professional cryptologists throughout Europe, as had happened in

Italy earlier. In some countries, this effort resulted in the establishment of so-called black chambers which engaged in the intercepting and decrypting of diplomatic dispatches on a daily basis. In England and France, these black chambers were operated by members of the same family on a semi-hereditary basis and posing as post officials. Strict loyalty and utmost secrecy were of the essence and there are very few reports of cipher clerks revealing their secrets. Any cryptanalytic expertise was considered a trade secret which was vital for the continuity of the business and therefore jealously guarded.

The undersigned writes about the black chamber in the Dutch Republic. As early as the revolt against Spain at the end of the 16th century, the Dutch had been intercepting Spanish military communications. They were proven successful in decoding partly through the bribing of a Spanish code clerk and partly through cryptanalytical effort. The first half of the 17th century saw various code breakers at work, mainly focusing on military communications. The most famous of these was the playwright Constantijn Huygens the Elder, who followed Stadholder Frederick Henry in battle as his personal secretary. Too little is known about possible contacts between these cryptanalysts, but it seems likely that no effort was made to ensure transfer of knowledge which may be explained by the relatively open political structure of the Republic which made keeping secrets difficult.

Therefore, in secret negotiations with foreign diplomats stadholders and grand pensionaries had to act on their own, which entailed the risk of being accused of high treason when things did not work out as expected. The political machinery afforded little opportunity for the long-term allocation of secret funds for a black chamber which implied that code-breakers were hired on an ad hoc basis at the discretion of individual statesmen. This code-breaker use is further exemplified by the temporary emergence of a black chamber between 1707 and 1715, during the War of the Spanish Succession and its aftermath. This chamber was manned by the personal secretary of Grand Pensionary Heinsius, Abel Tassin d'Alonne. D'Alonne, who had become familiar with code breaking while serving under his half brother Stadholder William III, focused on material intercepted at the post office in Brussels, which at the time was occupied by a combined Anglo–Dutch force.

Letters intercepted in the Republic proper were sent to Hanover to be decoded there. The reason for this transfer was to aid a political divergence with both the British and Hanoverians about the course taken in the Southern Netherlands. The important point to note is that only a few people were acquainted with d'Alonne's activity as a code-breaker, as the solutions never left the grand pensionary's office since both men worked in the same room. In the second half of the 18th century, another black chamber emerged in the Hague on the initiative of Pierre Lyonet, a cipher clerk in the service of the states general who excelled as a microscopist and an engraver of insects. Lyonet had been copying and storing French and Prussian diplomatic intercepts in order to have them decoded in London and he could not resist the temptation to try his luck on his own. He firmly believed that he was the first in the Dutch Republic to have ever been engaged in such activities and he was unaware that bishop Willes in London was assisted by a whole staff of translators and cryptanalysts.

Lyonet's work could easily go unnoticed since he already had been in the service of the states general since 1738. His cousin S.E. Croiset was called upon to assist him. Officially, Croiset was in the service of the post office. This formula lasted until the break-down of the Republic in 1795, with Croiset taking the place of Lyonet after his demise in 1789. Interestingly, Lyonet's activities as a code breaker also inspired him to improve the codes for the states general. Before that, Dutch cryptography was highly influenced by examples taken from literature, as can be seen in the application of Kircher's *Arca Steganographica* in the ciphers of the States General from 1658 onwards.

Jeremy Black writes about mail interception in 18th century Britain and the efforts to influence public opinion by the government. Mail interception focused primarily on foreign diplomats. It was carried out by a group of professional translators and code breakers working under the supervision of the secretary of the post office out of Secret

Service money after 1782 when the Foreign Office was created. The English black chamber originated in the 17th century when the mathematician John Wallis intercepted Stuart, French, and Spanish communications on behalf of parliament and later on behalf of William III. In 1715, the Hanoverian rulers took some of their own personnel with them from their black chamber at Celle. The collaboration with this black chamber remained in place until the personal union between Britain and Hanover ceased.

The appointment of the Reverend Edward Willes in 1716 marked the beginning of a veritable dynasty of code-breakers capable of reading the diplomatic traffic of all major and many lesser powers. Until 1746 the threat of a Jacobite overthrow was very real and it was supported by the threats of French and Swedish invasions. Therefore, domestic communications had to be monitored as well particularly in as much as members of the opposition were concerned and counter-insurgence strategies would have to include the influencing of public opinion, which was no straightforward matter. Censorship had been abolished and the government did not posses a newspaper of its own. Instead, the authorities had to rely on the releasing of favourable reports in both the foreign and the domestic press as well as the prevention of the publication of contentious information through lawsuits, particularly with reference to foreign policy.

The threat of legal action by the government had a pre-emptive impact. A case in point is the refusal of the Tory *Post Boy* in 1716 to print material offered by the Swedish envoy Gyllenborg about the British policy in the Baltic for fear of prosecution: a matter known to the government through the interception of Gyllenborg's reports. In the second half of the 18th century the threat of invasion and uprising waned, but the British Government remained dependent on public support for its foreign policy which was in contrast with the absolutist regimes in other states where foreign policy was considered the exclusive prerogative of the king and therefore never publicly debated. Of course, in this context, the need for reliable information, gained in importance.

Friedrich Bauer depicts the development of the rotor machine, a cipher machine based on a mechanisation and coupling of cipher disks. This machine was invented more or less simultaneously in The Netherlands, Germany, the US, and Sweden during or shortly after the First World War. In 1935 a modified version was adopted by the German military under the name ENIGMA and the machine was to play a key role in the German conquer of Europe five years later.

On introduction, the machine was considered practically unbreakable, due to its unprecedented key length. The Polish code-breakers nevertheless managed to penetrate German army traffic based on the exploitation of certain weaknesses in the way the machine was deployed and the use of key lists obtained through bribery. The Poles even devised a machine aimed at simulating the behaviour of the ENIGMA with various key settings, the BOMBA. After the Polish defeat in September 1939 this machine was transferred to England, along with all relevant documentation in order to assist the British cryptanalytical effort in Bletchley Park, which was to last throughout the war.

British mathematicians and engineers succeeded in making further improvements on both the machine and on cryptanalytical techniques which along with the capturing of key lists and a cipher machine on board of two German vessels allowed them to cope with the challenge posed by the introduction of a fourth rotor by the German navy in 1941. Bauer stresses that rotor machines, such as the SIGABA and the KL-7 or ADONIS did not share the design flaws of the ENIGMA and, consequently, were not penetrable in the same way. No rotor machine was ever theoretically unbreakable, however, because it was based on key repetition. A truly unbreakable cipher would have the characteristics of randomness and incompressibility, as may be the case with a one-time pad.

Jack Copeland fulfils a similar exercise for the Lorenz SZ 42, which was also broken at Bletchley Park, giving rise to the first computer. This machine, a teletypewriter used for communications between strategic command centres of the German military across Europe, was much more sophisticated than the ENIGMA and was only used for exchanges at the highest level of secrecy. With the

Siemens and Halske T52 and the Siemens T43, it belonged to a family of cipher machines devised for the protection of teleprinter traffic. They were not dependent on the rotor principle but rather on the use of a tape with additives: in the case of the T43 a one-time pad.

The Lorenz was eventually broken at Bletchley Park by building the Colossus: the first computer and usually seen as the result of Alan Turing's interest in electronics and his all consuming strife to build a 'decision machine'. Copeland shows that Turing, who interestingly was on a trip to the US when the actual work was done, played a more modest role than is generally believed. The decisive step from an engineering point of view that is, the large scale and controlled use of electronic valves as high-speed switches was first envisaged and implemented by Thomas H. Flowers.

Flowers, an engineer employed by British Telecom had been experimenting with electronics for over a decade. Moreover, the machine was programmed for the purpose of statistical calculations and devised by William Tutte. Turing had been involved in the breaking of 'Tunny', as the Lorenz was called, but at an earlier stage and his input had restricted itself to a pen and pencil method, involving a lot of guess work. Turing's ambition to build a 'logical engine' or 'decision machine' preceded the war by five years, but it was not instrumental in bringing about Colossus. The Colossus did serve for Turing and others as an example of how computers were to be built. Turing's professed interest in electronics, for instance, only occurred shortly after the war.

Silvan Frik writes the history of the only vendor of cipher machines that was commercially successful and remained so over the years: Crypto AG in Switzerland. This company was founded 1922 in Sweden as AB Cryptograph by Boris Hagelin with money from the Nobel organisation with the sole purpose of exploiting Arvid Damm's cipher machine. The success of this company was due to a large order placed by the Swedish army in 1926. Hagelin's key to success was his susceptibility to market demands. In 1930, the B-211 was launched, a portable electrical machine suitable for office-use. This machine was relatively expensive and was mainly sold to diplomatic services and big business.

In 1934, a small almost pocket-sized machine was designed for military purposes, initially known as C-34. This machine was hand-driven and was designed for use under harsh conditions. The rearmament ensured large sales in Europe, but Hagelin's break-through as a primary supplier of cryptographic devices came with the licensing of the C-machine to the US military in 1941. The American twin of the C-machine, the M-209, was manufactured at the Corona typewriter factory. With the navy, the army and the air force as customers, sales quickly reached fifty thousand.

In 1942, the Office of Strategic Services (OSS), ordered a new Hagelin machine: the BC-543 with a keyboard and an electric drive intended for office use. This machine would continue to play an important role in peacetime. Nevertheless, the first years after the war saw a steep decline in demand, but the Cold War was able to revive the business. In 1952 Hagelin transferred his company to Switzerland because of its tradition in precision engineering, its favourable tax climate, and the absence of export control. Initially, the attention was focused on the development of a telecipher machine in collaboration with Gretener. Later, much effort was put in the upgrade of the C-machine, the CX-52, which did not perform well.

Another device, a one time pad generator called CBI-53, performed better but was too expensive to be a commercial success. In 1955, however, the CD-55 was patented, a genuine pocket-size machine originally designed for the French police but later sold in large quantities. This machine as well as the rising demand of telecipher machines for diplomatic use proved a sound basis for expansion of the factory. The development of a small radio device for telecipher machines, equipped with a small antenna and using little electricity, was another asset since it suited the needs of the French Foreign Office, for instance, which wanted its embassies to be able to operate independently of the power supply or the communication facilities of host countries.

It also paved the way for further diversification, which became increasingly important for the firm as the age of the cipher machine was drawing to a close. In 1970 Crypto AG entered the age of electronics under a new director, Sture Nyberg, who had worked with the company for many years. Shortly after the T-450 was launched, the first fully electronic online text encryption unit came onto the market. This machine was widely used for both civilian and military purposes.

Another innovation was the CRYPTOVOX CSE-280: a device for digital voice encryption. The continuing success story of Crypto AG is ample illustration of Kerckhoff's maxim that the secrecy of a communication line solely depends on the secrecy of its keys. The cipher system or device may well be known to enemies. This holds true for the age of cipher machines, as well as for the age of electronics and computers.

Matthew Aid writes about the deployment of Soviet signals intelligence (SIGINT) capabilities, mainly during the Cold War. He traces the origin of the Soviet code-breaking back to 1921, when the Cheka formed a cryptologic department, drawing its personnel mainly from the Tsarist black chamber that had rendered good service before the Revolution. The new department focusing on diplomatic traffic gained its first successes against German and Turkish diplomatic ciphers soon afterwards and was reading the diplomatic traffic of fifteen nations by 1925. Stalin's 'Great Terror' led to the execution of most of its staff during the latter part of the 1930s, including the successful founder of the department Gleb Bokiy who was considered politically unreliable.

Due to the outbreak of the war with Germany, efforts were made to regain strength mainly by recruiting academics. The Red army and navy had SIGINT organisations of their own, which did not collaborate well. Therefore, Soviet SIGINT capabilities were brought under direct control of the Peoples Commissariat of State Security 5th Directorate from November 3, 1942 onwards under General Shevelev. The result was a successful monitoring of German military activities in the air, sea, and land during the latter part of the war.

The military branch regained independence after the end of hostilities, resulting in a revival of much of the animosity between civilian and military intelligence that had existed before. Unfortunately, expenditure on civilian SIGINT was cut down and little efforts were made to invest in research and development, as was the case in the US which resulted in a technological backlog that was to last throughout the Cold War. Considerable results were gained, however, through conventional espionage, assisting SIGINT operations, such as the burgling of embassies in order to steal code books, or the bribing of American SIGINT personnel.

The most spectacular example of the last was the so-called Walker spy ring which provided the Soviets with cryptographic material for nearly twenty years in such quantities that it could easily have led to serious losses for the US Navy. Another important asset was the fielding of a new generation of domestically produced high-frequency intercept systems shortly after the end of the war based on a captured German design. This version allowed the Soviets to monitor virtual all NATO activity, mainly through traffic analysis and provided the Soviets with an early warning system in case of a pending nuclear war. Therefore, the Soviets were far from powerless, notwithstanding their inability to keep up with the pace of technological progress in the west.

Joseph Fitsanakis gives a brief account of the history of it National Security Agency, the American counterpart of the KGB's 5th Directorate in a manner of speaking. Unlike Tsarist Russia, the US had no long-standing tradition of code-breaking and, consequently, had been poor in the deployment of ciphers and of codes. By 1890 both the US army and navy had established small intelligence organisations, however, which were thoroughly under-funded and understaffed when World War I broke out in April 1917.

A newly-created intelligence section of the general staff was set up five days after America's entry into the war in order to fill in gaps of intelligence gathering. One of its branches was MI8, a cable and telegraph section, which was soon to become America's first full-grown civilian code-breaking organisation. Under the inspiring leadership of Herbert O. Yardley, the section decrypted eleven thousand foreign cable telegrams in nearly thirty months, mainly from Germany and from Central and South America.

There is no indication that the intelligence provided by MI8 greatly influenced American diplomacy during the negotiations at Versailles, and after the war Yardley's organisation was cut back from over three hundred in 1918 to less than twelve in 1924, which did not prevent Yardley from being successful against Japanese codes during the Washington Conference in 1921. However other major powers were untouched by these efforts in part because telegraph companies were no longer willing to supply the necessary intercepts. Not very surprisingly, Yardley's black chamber was closed in 1929 by the State Department, leaving the US without any code-breaking expertise.

The greatest damage was done to the army's Signal Corps, responsible for the provision of up to date cryptographic information. Therefore shortly after, a new branch was established, the Signals Intelligence Service (SIS), with cryptanalytic research being one of its functions. Under direction of William Friedman, the SIS elevated cryptographic practises in the army, and its methodical training program was at the root of the successes against enemy diplomatic codes at the outset of the war against Japan: better known as Purple. In 1949 the SIS assumed the co-ordination of the strategic activities of all US SIGINT organisations under the name of Armed Forces Security Agency (AFSA), and thus became a direct forerunner of the NSA.

In 1950, AFSA was still struggling to assert its authority and proved unable to predict the Korean War or to contribute much to it. The creation of the highly centralised NSA in 1952 was a direct response to this disappointing performance of the American SIGINT agencies which was meant to support well co-ordinated global policies in accordance with America's role as a superpower. Unlike its Russian counterparts, the NSA, as a matter of policy, heavily invested in computer research ultimately leading to the deployment of the Stretch supercomputer in 1962.

During the 1950s, the NSA also accomplished a spectacular augmentation of its intercept capabilities. These efforts were almost exclusively directed against the Soviet Union, leaving room for blind spots in other parts of the world, such as in the Middle East, where the Suez crisis would occur in 1956. The 1960s saw a further expansion of the agency, which by 1969 was to become America's largest and costliest intelligence agency with one hundred thousand employees and an estimated budget of two billion dollars.

The 1970s saw an increasing importance of satellite surveillance systems which were brought into orbit in collaboration with NASA and the National Reconnaissance Office (NRO). The satellites were a key component of a global, automated interception and relay system, codenamed ECHELON, fielded in collaboration with the UK, Canada, Australia, and New Zealand on the basis of an agreement stemming from the Second World War. Except from a comprehensive successful counterintelligence operation against the Soviets, known as Venona, little is known about the NSA's results and possible failures and even the scope of Echelon remains clouded in mystery.

The collapse of the Soviet Union in 1990 left the NSA without a mission, except for economic espionage against friendly countries which resulted in political tensions with the European Union and, in the US itself, to a revival of the debate about the NSA's possible role in the surveillance of American citizens. The organisation's budget was reduced substantially, and efforts were made to redirect priorities, nuclear proliferation being one of them. The future of the NSA is far from clear. The spread of fibre optic systems, combined with the increasing prevalence of strong cryptography, severely reduces its capability to monitor and the sheer increase in e-mail traffic in recent years seems to have a similar effect.

Bart Preneel investigates the development of contemporary cryptology, from the predecessors of the Digital Encryption Standard (DES) during the 1950s until today. Cryptology plays an essential role in the protection of computer systems and communication networks and civilian applications have increasingly gained in importance since the 1960s. For over thirty years, cryptologic research has slowly developed into a full-grown academic discipline. Progress depends on the publication of algorithms and proofs, leaving less and less room for the secrecy that has accompanied military research over the past.

Preneel dates the origin of this development to 1949 when C. Shannon published a mathematical proof that a perfectly random key sequence renders perfect security if the key is exactly as long as the message. This so-called Vernam scheme had been applied during and after the Second World War in various Soviet diplomatic cipher systems, which proved far from unbreakable for US cryptanalysts in the context of Venona. These results were due, however, to a reuse of tapes proving that errors in the use of a cryptosystem can be fatal even if the system is theoretically secure. This error pointed to a serious weakness in the Vernam scheme, however, because application depended on the exchange of huge volumes of cipher tapes which puts a strain on logistics.

The problems of key management and key exchange moved to the fore with the advent of the computer. Encryption was either left to stream ciphers, operating on the plaintext character by character or on block ciphers, operating on plaintext strings, which were sufficiently strong to defy attacks given a certain amount of computing power. This approach was firmly rooted in tradition, but had flaws that were particularly troublesome in computer networks. First of all, there was no possibility of exchanging keys over a network without taking the risk of interception. To make things worse establishing the identity of the other party was not straightforward because these so called 'symmetric' keys could easily be used to impersonate the original sender.

Public Key Cryptography, independently invented in 1976 by Diffie and Hellman and Merkle, was devised to solve both problems at once. In Public Key Cryptography, different keys were used to encrypt and decrypt messages. The public key was deposited somewhere on the web and could be used by anyone who wanted to send a message, but this message could only be decoded with the private key of the owner which never left the original location. The idea behind this method was based on an observation from number theory which says that it was much easier to multiply primes than to decompose them if these primes were of sufficient length.

Public Key Cryptography turned out to be the most important innovation in cryptology since the advent of the computer and it took only a decade to become an indispensable technology for the protection of computer networks. The irony of it all is that cryptology as a science has been of limited importance in achieving this breakthrough even as it successfully developed various models or approaches to think about the security of encryption algorithms. The information theoretic approach of Shannon has already been mentioned. The so-called 'complexity theoretic' approach departed from an abstract model of computation, for instance a Turing machine, and assumes that the opponent has limited computing power within this model. These approaches exist side by side with a more practical, or 'systems-based' approach, focusing on what is known about weaknesses and strengths of any algorithm in the context of a given configuration. The science of cryptology has never been able to prove that the factoring of primes is indeed as hard as it is supposed to be.

1.8 COMPUTER SECURITY

The fourth part of this book is on issues of computer security. Jeff Yost writes about the sense and nonsense of computer security standards, such as the *Orange Book*. He traces the origin of the quest for security standards back to the US Department of Defense's worries about security in time-sharing and multitasking environments during the 1960s. The DoD had played an important role, along with certain privileged companies such as IBM as well as high-level research institutions such as MIT, in the early development of computer technology during the 1940s and 1950s.

This development had taken place in private and relatively secure environments which were mainly protected by controlling physical access. The introduction of time sharing and multi-tasking made clear that there was no way of enforcing the strict classification of DoD-documents in degrees of confidentiality in a sophisticated computer environment. In October 1967, the Defense Science Board commissioned a task force, under the chairmanship of Willis Ware, to describe the problem. On February 11, 1970, this task force published its report, which stated among other things that providing satisfactory security control was in itself a system design problem.

In 1972, the US air force followed suit with a report written by James Anderson, developing the concepts of the security kernel and the reference monitor. In 1973, a first model for developing security policies was by Bell and LaPadula, focusing on the needs of the military and bureaucracy. In 1983, these and other initiatives acted as building-blocks for the *Orange Book*: the DoD's first rating system for establishing the level of security of any given computer system. In later years, there were an entire 'Rainbow Series' of security standard books that were being followed both in the US and in Europe and ending in 1996 with the *Common Criteria*.

These more recent rating systems were developed to accommodate the needs of network-computing and business life and privacy-sensitive civilian institutions, such as health care. The adoption of rating-systems like these outside of government use has been growing in recent years, notwithstanding the reluctance of organisations not bound by law. Interestingly, the US government has been far less successful in enforcing standards for cryptography. The introduction of DES in 1976 by the National Bureau of Standards happened with the specific purpose of promoting the use of weak cryptography for civilian use by limiting the key size. This effort backfired because of the rise of Public Key cryptography: a cryptographic algorithm of unprecedented superiority developed by academics unrelated to any government institution and marketed by private enterprise. This invention came to be the de facto world-wide standard for secure communication during the late 1980s and early 1990s against all efforts to block the export of sophisticated encryption technologies.

Dieter Gollmann writes about security models. A security model is a formal description of a security policy that a system should enforce. It is used as a yardstick in the design process of a computer system for determining whether it fulfils its security requirements. Security models are based on the state machine model. A state is an abstract representation of a computer system at any given moment in time. A security model represents a machine in an initial, secure state. The possible state transitions are specified by a partial state transition function defining the next state depending on current state and input. A "Basic Security Theorem" can be formulated when it is clear that all state transitions preserve the initial security of a particular system.

Security models are already recommended in the aforementioned report J. Anderson has written for the USAF in 1972. Various models were developed, but the Bell–LaPadula model from 1973 remained the most influential because it was recommended in the *Orange Book* and because it was applied in Multics. The BLP model reflects the multi-level security policy of the military, using labels such as 'unclassified', 'confidential', 'secret' and 'top secret'. The model introduces a reference monitor deciding whether to deny or to grant access on the basis of a user's clearance. In 1987 the BLP model was severely criticised by J. Maclean because it allowed a state transition which downgraded all subjects and all objects to the lowest security level and because it entered all access rights in all positions of the access control matrix and would still label a system as 'a secure state'.

Bell's counter argument was that if the requirements called for such a state transition, it should be possible to express it in security model. At the root of this disagreement is a state transition that changes access rights. Such changes would be possible within the general framework of BLP, but the model was intended for systems that are running with fixed security levels or to put it differently, it is intended for systems that are in a state of 'tranquility'. The BLP model had other limitations as well. It did not sufficiently capture multi-level security requirements for relational databases and neither did it capture the security requirements for commercial security policies. This flaw was pointed out by David Clark and David Wilson who argued that in business applications the unauthorised modification of data constituted a much bigger problem than a possible breach of confidentiality. They advocated the use of a specific set of programs for the manipulation of data items by privileged users working, if possible, under the condition of separation of duties.

Behind this debate, a technological shift can be noticed. BLP clearly refers to a world of general purpose, multi-user operating systems; Clark and Wilson refers to networks and application oriented IT systems. In parallel with the development of models for existing security policies, another line of work developed which explores the theoretical limitations of security models. Its purpose is the analysis of the intrinsic complexity of access control or the provision of generic frameworks for analysing information flow within computer systems. Early examples of these models are the Harrison–Ruzzo–Ullman model, the Take–Grant model from 1976, and a more recent example is the research on Execution Monitoring by Fred B. Scheider dating from 2000. Current work focuses on decentralised access control and the defining of flexible languages for expressing security policies without prescribing the types of policy that can be enforced.

Bart Jacobs, Hans Meijer, Jaap-Henk Hoepman and Erik Poll deal with the subject of programming transparency as a way of achieving of computer security. They trace the efforts to investigate computer security back to 1961, when Vyssotsky and McIlroy conceived a game for the IBM 7090 in which self-replicating computer programs tried to destroy each other. Starting out as a merely academic pastime, exercises like this gained importance because of the rise of multi-programming during the late 1960s. Efforts to improve programming transparency, as manifesting itself after the proclaiming of the software crisis in 1968, did not address security issues separately because security was perceived as a by-product of correctness. Ironically, computer scientists who did address such issues, such as the authors of the *Orange Book* occupied themselves mainly with security policies and access control.

The inadequacy of this approach became obvious only during the 1990s due to the spread of viruses and worms on the Internet and other exploiting bugs in programs. Jacobs and his colleagues believe a multi-faceted approach was necessary, and they consider the use of open software to be an important pre-condition for improving computer security. Surprisingly, they recommend bringing the development of 'secure' software libraries into the hands of academic institutions under supervision of the state.

Laura de Nardis explains how the Internet protocol TCP/IP was initially designed for a closed community, such as the military and academia. Security hazards came to the fore after the adoption of the Internet by the general public. The sudden occurrence of the Morris-worm on 2 November 1988, infecting thousands of Unix-computers mainly in the United States, heralded a new era of public awareness. The attack was well planned by Robert T. Morris, son of a chief scientist at the National Computer Security Center to illustrate inherent Internet vulnerabilities and the inadequacy of prevailing network security measures.

Shortly afterwards, the Computer Emergency Response Team was founded to monitor irregularities on the Internet. Other, less benign attacks were to follow, leading to a rise of commercial security products, such as firewalls during the 1990s. The introduction of Virtual Private Networks to protect businesses and other organisations from intrusion was another approach which required strong encryption which, however, led to a fierce debate between policy makers who feared proliferation of military sensitive technologies to hostile countries and providers of encryption technology, lingering on until the turn of the century. This objection did not withhold viruses and worms from becoming legitimate plagues, causing serious disruptions of the Internet in 2001 (Code Red, Nimbda), 2002 (Klez), 2003 (Slammer, Blaster) and 2004 (My Doom, Bagle, Sasser).

Additionally, fear of cyber terrorism led to the development of a "National Strategy to Secure Cyberspace" by the US government, stressing the nation's dependency on information infrastructures. The recent growth of wireless Internet access has added a new dimension to the vulnerability of Internet use, and the numbers show that security incidents are rising annually. DeNardis does not rule out, however, that the introduction of a new Internet Protocol, IPv6, may result in an improvement in the near future.

Susan Brenner covers the issue of computer crime. She describes a development starting with the introduction of mainframe computers from conventional crimes, committed by insiders, often disaffected employees, to true computer crimes mainly committed by outsiders in the era of network computing and the Internet. The first wave of such activity emerged during the 1980s from the hacker community to make clear that legislation was lagging behind technological developments; the main problem shown was the 'virtual' character of gaining access which had never before been demonstrated.

Initially, these activities were relatively benign. During the 1990s, however, organised crime became increasingly involved on a world-wide scale, engaging in such diverse activities as online theft, online fraud, identity theft, and the use of malware for the purpose of extortion. These crimes were difficult to combat legally not only because of the unprecedented scale but also because of the international character of computer crime which demanded the harmonising of legislation and the collaboration of criminal investigation officers in the countries involved. The chapter ends on a pessimistic note. Brenner signals a lack of energy in the arena of international policy-making and law to combat cyber-crime. Unfortunately, the international crime scene is more energetic. There are now new types of organised crime, less hierarchically structured and less rooted in local folklore, or to put it differently more fluid and harder to combat than ever before.

Margaret van Bienc-Hershey writes about IT-security and IT-auditing. IT-auditing came into existence around 1960 when accountants were initially confronted with important financial information that was being digitally stored. New, computer literate auditors were needed to assist the accountant in obtaining the evidence necessary to approve the financial statements made by an enterprise. They were called Electronic Data Processing auditors (EDP auditors) because during those early days of ubiquitous computer use the main issue was about the storage of data. No major changes were made in the structure of the work processes within any organisation; but the output increased with fewer people. Input was made through punch cards, and magnetic tapes were used for back-up during the night.

The introduction of the IBM 360 in 1964 meant that computers became much faster, through the added features of multitasking and paging which made use of core memory which was suddenly much more flexible and efficient then ever before. The control on completeness and correctness could easily be done by the business unit responsible for the process. It was simply a matter of error detection. Audit-software programs were written to check the integrity of the master files through hash totals.

IT-auditing is primarily an audit of the computer centre's organisational procedures for carrying out production processes. In approximately 1970, this situation changed dramatically through the introduction of storage on disk, on-line data entry, and data base management systems which meant that the same data sets became accessible throughout a company and that the integrity of data could no longer be checked on a business unit level. Data base administrators assumed company-wide responsibilities and IT-auditors had to occupy themselves with procedures for data entry and data format which lay far beyond the scope of the computer centre.

Between 1972 and 1974, research initiated by IBM and executed by MIT, TRW systems, and IBM's Federal Systems Division itself resulted in a trail blazing series of technical reports about data security. The scope of IT-auditing was broadened with the audit of development of business systems and the audit of business systems controls. The IT-auditor reports directly to the management of the company and participates in the design of data communication processes as well.

The arrival of the PC and local area networks during the 1980s caused new data integrity problems, however, because programs and data could now, once again, be stored on the business unit level. The rise of the Internet added new security threats because it rendered the business networks vulnerable for attacks from outside. From 1990, the IT-auditor had to be concerned with new areas such as encryption and key management and also with the enforcement of privacy laws. The IT-auditor, then, increasingly assumes the role of an advisor to the management on security policy issues which does not mean that he is fully capable of fulfilling this new task. The poor quality of current Internet protocol, which makes it impossible to establish where a message comes from, prohibits the staging of fully effective security measures. The poor, or even absent, security-architecture in PC's adds to the problems. It is Van Biene's firm conviction that the computer industry should take responsibility for this issue.

1.9 PRIVACY AND EXPORT REGULATIONS

The fourth section consists of three contributions about privacy and export regulations. The first chapter in this part is written by Jan Holvast and deals with privacy or 'the right to be left alone' as it was first defined by Samuel Warren and Louis Brandeis in a famous article written in 1891. Privacy is a basic human need second only in importance to the need for safeguarding physical integrity and privacy issues can be traced back to biblical times.

The American constitution refers to privacy without using the term but by way of limiting the right of the state to enter citizens' homes. The concept acquired a broader meaning around the turn of the century with the rise of gossip journalism and the taking of pictures without consent. In 1928 a further dimension was added when federal investigators started wiretapping communications of citizens without a warrant under the pretext that wiretapping did not involve physical trespassing and was therefore fully constitutional. This reasoning did not hold and thereby, the right of the citizen to prevent the collection of data pertaining to him was firmly established.

The application of computer technology and the amassing of large volumes of data both by government agencies and by big business that goes with this area gradually changed the equilibrium that had existed before the war. Citizens have had no way of accessing data collected without new legislation. This issue sparked a political debate which resulted in a federal privacy act in 1974.

Unfortunately, efforts to curb the collection of data by private enterprise were hampered by the fact that the Constitution protected only the rights of the citizen against the state, but not against businesses, large or small. The development in Europe was somewhat different because the basis for future privacy acts was laid in 1950 with the European Convention for the Protection of Human Rights and fundamental freedoms. The information society resulted in a similar infringement of privacy as that found in the US and a similar effort to mend affairs through privacy acts in various member states culminated in a European Directive on Data Protection in 1990.

This Directive established a set of guiding principles for data collection, applicable on both private enterprise and government agencies. The core idea is that data collection should be purpose-bound, limited in the sense that these data should not be made available to third parties without consent, and that the individual should have the right of access without excessive costs. Regulatory agents, or data commissioners, are put in place to ensure that governments and business practises are in accordance with this law. In 1997, a second European directive was adopted, specifically related to the protection of privacy in the telecom sector which was a response to the emergence of spyware and the increase in unsolicited communications for marketing purposes, both occurring on the Internet.

In the US similar concerns had taken the form of self-regulating efforts by industry. The effect of these privacy laws seems limited, however, and insufficient to end further infringements. The driving forces behind the ever growing amassing of data are, in terms of money and power, too massive to be halted by legislation. A second, more abstract problem is the difference between information and data. Data can easily be protected, but information, that which is derived by putting data together, cannot be easily protected. In the end, it is information that constitutes the threat to privacy, not data.

Whitfield Diffie and Susan Landau explain why the tight US export control regulations for cryptography, valid for over forty years, were finally released at the end of the Clinton administration very much against the declared interest of the NSA.

Shortly after the Second World War the export of cryptography was put under the surveillance of the Munitions Control Board, a section of the state department which monitored the export of military goods with the objective of protecting national security. This Board acted on the instigation of third parties, in the case of cryptography, on the advice of the NSA or its predecessor.

During the early part of the Cold War, this method made sense because the demand for cryptography came almost exclusively from foreign governments in order to serve either diplomatic or military purposes. The situation changed with the rise of network computing during the last quarter of the 20th century. The importance of civilian use of cryptography increased, especially in the field of banking and commerce. The export control was retained nevertheless because it was considered an effective instrument to promote the deployment of weak cryptography abroad but also for civilian use in the US for reasons of crime investigation.

This use was detrimental to the interest of the US computer industry, increasingly challenged by foreign competition. After a public debate that continued for over a decade, control measures were relaxed in 1996 and finally abolished in 1999 as part of the election campaign of Vice-President Al Gore who sought support from Silicon Valley. Diffie and Landau do not believe that expediency tipped the coin altogether. The proven inability to prevent export of cryptographic algorithms in written form, such as Pretty Good Privacy (PGP), because of the Fifth Amendment, indicated that the existing export policy found little justification in the constitution and, therefore, had to change.

Finally, the rise of Open Source Software provided the rest of the impetus. Open Source Software is generated by a conglomerate of loosely associated programmers, who are scattered around the world. This allows anyone to add strong encryption modules to existing programs whenever the need requires the additions. Export control measures had always been targeted at companies, treating software as a finished and packaged product. The Open Source movement managed to make this approach largely ineffective.

Andrew Charlesworth writes about the consequences of the crypto controversy for the privacy debate predominantly in US and in Europe. Until 1970 there had been little public or academic interest in cryptology and organisations such as NSA have found slight difficulty in controlling cryptological research since previously this concern took place in the context of military institutions or government laboratories. All is changed now with the spread of personal computing which creates a need for cryptography as a privacy tool which in turn has stimulated a new wave of a cryptological research taking place in the context of computer science departments and practised as an academic discipline.

The watermark of academic research is the publication and subsequent scientific debate of results which potentially undermines any government monopoly in this field. Initially, the NSA focused on discouraging the publication of cryptological research in the name of national security and prohibiting export. The collapse of the eastern block in 1989 made this approach obsolete, however. At the same time, the rapid expansion of the Internet made the public availability of strong encryption tools commercially viable and a new political issue connected to the privacy debate. In 1994, the US Government responded by removing encryption software from the list of military goods that could only be exported with the consent of the state department. At the same time it also introduced the principle of key escrow. Key escrow entailed the obligation of commercial encryption suppliers to deposit keys with the law enforcement agencies or, worse still, the obligation to install so-called trapdoors in any encryption device put for sale thus allowing NSA to read encrypted communications.

This policy change was defended in terms of law enforcement and counter terrorism, but it also brought all communications under surveillance of the state which meant a huge encroachment on the privacy of American citizens. Unfortunately, key escrow made American encryption products unattractive for buyers outside the US who had something to hide from American authorities, such as governments with independent views of international affairs or businesses with American competitors. US efforts to find general acceptance of these measures through negotiation in international bodies, such as OECD failed because most countries believe that the NSA was using its large intercept capabilities mainly against its former allies for economic espionage.

Interestingly, the opposition to the American proposals led to a liberalisation of encryption market throughout most of Europe and even in countries that had been extremely restrictive in the past, such as France. After 2000 the effort to control the proliferation of encryption technologies dwindled in most countries, but this lessening does not mean that the concern for privacy is no longer warranted. With the introduction of its so-called Magic Lantern, the FBI is now able to monitor the on-line behaviour of any suspect in the name of law enforcement which certainly illustrates a general tendency of law enforcement agencies to evade encryption through the instalment of spyware. Another and perhaps more important threat is the use of strong encryption to protect intellectual ownership, as is the case in the Digital Copyright Millennium Act which makes it virtually impossible to access information without being known to the owner, which if it were possible to do would be an encroachment of privacy without precedent.

1.10 INFORMATION WARFARE

The sixth part of the book consists of one contribution that really does not fit into any of the other categories and that is Dan Kuehl's chapter about Information Warfare. Kuehl shows how military analysts take into account the growing strategic importance of information systems, both civilian and military, for warfare. He sees three vital areas in which the information revolution is shaping the future of national security. The first area is about protecting computer-controlled critical infrastructures from malevolent acts and attacks. The second is about the growing importance of information operations to military affairs, and the third is about the struggle for global influence in a political and ideological sense.

The threat to critical infrastructures or, more specifically, command and control centres is not new. The bombing campaign against Germany was an effort to disrupt industrial plants, and the railway system served as an example of the former. The bombing of Turkish telegraph nodes by General Allenby during the campaign in Palestine in 1918 illustrates the latter. What is new, however, is the growing use of supervisory control and data acquisition technologies to monitor the status and to control the operation of a segment of this infrastructure, such as a rail network or an electric grid.

These can be attacked without much effort, from anywhere in the world by only a handful of people who do not even have to be in the same place. Information operations aim at exploiting the vulnerabilities of the electronic infrastructure. Psychological warfare, operations security, military deception, electronic warfare, and computer network operations are all part of information operations. The operations theatre itself merits a closer examination, however. The physical dimension of an information environment is made up of the infrastructures, networks, and systems that store, transfer, and use information. The information that is, the content is itself the second dimension.

The third dimension is the cognitive that is, how the information is perceived. Information operations aim at the manipulation of data, for instance for the purpose of military deception or psychological warfare which means that they focus on content but not on infrastructure. The third dimension comes closer to the traditionally known propagandistic aspects of warfare with the notable difference that the propagation of ideas, views or perspectives through the Internet is hard, if not impossible, to control. Information operations have acquired a prominent role in military theory because it may result in a rapid disruption of enemy command and control centres or supply lines. The Chinese in particular seem to envisage information operations in the context of asymmetric warfare against the West by allowing poorly equipped parties to gain military successes against an otherwise superior enemy. Kuehl argues that existing strategic concepts, such as those developed by Von Clausewitz are still viable to come to grasp with these new threats. He does emphasise, however, that the military cannot do its job alone; any strategic effort to protect a national infrastructure should include the civilian sector as well.

1.11 CONCLUDING REMARKS

The information society is based on an unprecedented civilian deployment of security tools and technologies which is insufficiently weighted in the current accounts of the impact of the new information and communication technologies, such as the Internet. On the contrary, the advent of the Internet has inspired many almost utopian visions of society. The Internet is supposed to bring an unrestricted flow of information. Eventually this influx will lead to the erosion of the role that traditionally has been hierarchically structured within organisations. Fairly typical is a statement by Douglas Cale, National director of Computer Assurance Service Practice of Deloitte & Touche who says: "The first characteristic of sound knowledge management is collaboration as opposed to organizational hierarchies. A second is openness as opposed to a separation of functions (...). Traditional structures such as entry controls, data security, and information classification are barriers to creating knowledge and managing it well".[7] This statement may all too well be true but it does not make such barriers superfluous.

Security tools have a long history but they have always been applied on a limited scale, in the context of hierarchically structured organisations, such as the military, within bureaucracy, or within corporate structures. Previously the deployment of security tools was in the hands of organisational apparatus that already obeyed rules of confidentiality, integrity, and availability. This may no longer be the case and it seems unlikely that technology can fully compensate for that lack. The spread of malware through the Internet proves that present computer security practises are insufficient. The quest for provable correctness of software has not been able to turn the tide thus far, perhaps because Open Source software is insufficiently backed by government policies.

Cryptographic protocols seem to be functioning well, but the scientists have not been able to prove why this is the case. Biometrics systems lag far behind the expectations of policy makers but improvement is likely due to the massive deployment of inferior technologies that is now underway and the problems that this situation will cause in the nearby future.

The capacity of policy makers to steer technological developments is limited which can be learned, for instance, from the relaxation of export regulations for encryption software after many years of political strife. This policy change was as much a result of political expediency as of the advent of open software, which made it possible to export unfinished products and include encryption modules abroad. The liberalisation of the use of encryption software did not eliminate all threats to privacy, however. The Digital Copyright Millennium Act for instance, makes it virtually impossible to access any information without being known to the owner, which of course would be an encroachment of privacy without precedent.

More generally, policy makers all over the world have been reluctant to develop a legal regime that meets the necessities of the information age. This short-coming can be seen, for instance, in the fight against computer crime especially in as much as this requires international co-operation. Privacy laws have been proven unable to prevent the occurrence of massive data-warehousing for commercial purposes because the enforcement agencies that have been created everywhere are not strong enough to turn the tide.

Moreover, the continued existence of large signals intelligence establishments as well as the rumours of economic espionage seem to suggest that governments, even those that ascribe to the rules of fair competition, are not always playing legally and fair. Under these circumstances, a co-ordinated effort to protect the information infra-structure of democratic countries seems unlikely.

[7] Quoted in: Donn H. Parker [24, 7,8].

REFERENCES

[1] J. Agar, ***The Government Machine***, MIT Press, Cambridge, MA (2003).

[2] M.M. Aid, C. Wiebes (eds), ***Secrets of Signals Intelligence during the Cold War and Beyond***, Frank Cass, London (2001).

[3] R. Anderson, ***Security Engineering. A Guide to Building Dependable Distributed Systems***, Wiley, New York (2001), pp. 200–203.

[4] C. Beavan, ***Fingerprints. The Origins of Crime Detection and the Murder Case that Launched Forensic Science***, Hyperion, New York (2001).

[5] D. Bell, ***The End of Ideology: On the Exhaustion of Political Ideas in the Fifties***, Free Press, New York (1965).

[6] D. Bell, ***The Coming of Post-Industrial Society. A Venture in Social Forecasting***, Basic Books, New York (1973).

[7] J.R. Beniger, ***The Control Revolution. Technological and Economic Origins of the Information Society***, Harvard University Press, Cambridge, MA (1986).

[8] W.E. Bijker, T.P. Hughes, T. Pinch (eds), ***The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology***, MIT Press, Cambridge, MA (1987).

[9] E. Black, ***IBM and the Holocaust***, Crown Publishers, New York (2001).

[10] K. Breckenridge, *The biometric state: the promise and peril of digital government in the New South Africa,* Journal of Southern African Studies 31 (2005), 267–282.

[11] J. Caplan, J. Torpey (eds), ***Documenting Individual Identity: The Development of State Practices in the Modern World***, Princeton University Press, Princeton, NJ (2001).

[12] A. Chandler, ***The Visible Hand: The Managerial Revolution in American Business***, Harvard University Press, Cambridge, MA (1977).

[13] J. Ferris, *Airbandit C31 and strategic air defence during the first Battle of Britain, 1915–1918*, ***Strategy and Intelligence. British Policy during the First World War***, M. Dockrill and D. French, eds, Hambledon, Condom (1996).

[14] M. Foucault, ***Discipline and Punish: The Birth of the Prison***, Penguin, Harmondsworth (1980).

[15] D. Gollmann, ***Computer Security***, Wiley, Chichester (1999), pp. 5–11.

[16] A. Jones, G.L. Kovacich, P.G. Luzwick, ***Global Information Warfare. How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages***, Auerbach, Boca Raton, FL (2002), p. 20.

[17] D. Kahn, ***The Codebreakers***, Macmillan, New York (1967).

[18] G.E. Kurtz, ***Willem III en Amsterdam, 1683–1685***, Kemink, Utrecht (1928), pp. 95, 98, 107–109.

[19] S. Levy, ***Crypto. How the Code Rebels Beat the Government-Saving Privacy in the Digital Age***, Penguin, Harmondsworth (2001).

[20] S. Levy, ***Hackers: Heroes of the Computer Revolution***, Penguin, Harmondsworth (2001).

[21] F. Machlup, ***The Production and Distribution of Knowledge in the United States***, Princeton University Press, Princeton, NJ (1962).

[22] D. MacKenzie, J. Wajcman (eds), ***The Social Shaping of Technology***, Open University Press, Buckingham, Philadelphia (1999), pp. 10–11, 142–143.

[23] A. Menne-Haritz, ***Business Processes: An Archival Science Approach to Collaborative Decision Making, Records, and Knowledge Management***, Kluwer Academic Publishers, Boston, Dordrecht, London (2004).

[24] D.H. Parker, ***Fighting Computer Crime, a New Framework for Protecting Information***, Wiley, New York (1998).

[25] E.S. Raymond, ***The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary***, O'Reilly, Sebastopol, CA (1999).

[26] B. Schneier, ***Beyond Fear***, Copernicus Books, New York (2003).

[27] S. Singh, ***The Code Book. The Science of Secrecy from ancient Egypt to Quantum Cryptography***, Fourth Estate, London (1999).

[28] A. Toffler, ***The Third Wave***, William Morrow, New York (1980).

[29] A. Westin, ***Privacy and Freedom***, Atheneum, New York (1967).

[30] S. Williams, ***Free as in Freedom: Richard Stallman's Crusade for Free Software***, O'Reilly, Sebastopol, CA (2002).