The Control of Technology by Nation State: Past, Present and Future - The Case of Cryptology and Information Security

E Filiol

Operational Virology and Cryptology Laboratory
ESIEA, Laval, France
E-mail: filiol@esiea.fr

Abstract: *Since the fifties, strong controls have been enforced to prevent the spread of military-grade technology or dual use technologies and, later, especially of Information Security science. These controls originally focus on homeland and international security purposes. But the fall of the Soviet bloc has changed the situation. The enforced controls now aim at organizing an economic dominance of a very few Nation States whose real intent is to organize the strategic dominance over the rest of the world. This paper explains how controls have been organized by the four major actors: Nation State, Industry, Academics, and Hackers.*

Keywords: *Cryptography, Dual Technologies, Export Control, Economic Dominance, CoCom, Wassenaar Arrangement, Strategic Dominance.*

Introduction

Since the end of World War II (in fact, in the mid-40s), technology has been under strict controls especially regarding the export towards foreign countries. Although it concerned the military world at the very beginning—especially in the emerging context of the cold war era—this concerned many other technologies as well. The public opinion is totally unaware of that. The goal—which is understandable and compelling in itself—was the need to preserve, through the control of exports, the sphere and the regal power of the States which have an obligation to protect their interests (in particular military as well as economic ones), their citizens, and their values. Terms like CoCom, Wassenaar, counter-measures, cryptology laws and regulations, backdoors illustrate this trend.

But things have gone much further and in a more pernicious way, thus preparing almost the absolute control by a very small number of entities (states and multinationals) on everything related to computer security and Internet. The purpose of this paper is to present the dark side of the computer industry, computer security and, through it, of the Internet; to examine how a game of chess started in the 40s could end; and to show the dramatic consequences, both at the strategic level for the Nation states and with regard to the issue of freedom for citizens.

To illustrate this and without loss of generality, the field of information technology, security, in other words, to be fashionable, the cyber defense and all areas that depend on that particular domain are considered, as an illustration. But concerns should extend in fact to any possibly sensitive technology known or said to be ‘dual’. The word ‘dual’ should raise questions for any global citizen especially in a context of fierce international economic competition and of the rise of terrorism, both in the classical sense but also the economic one. The information and the systems that process it are THE most critical dimension, which, nowadays, determines

and is at the heart of everything: whoever is the master of information is the ruler of the world. The proposed restriction to the field of information technology is therefore highly relevant.

The paper is organized as follows. The second section presents the four different players who are involved in one way or another in the different controls in place. The third section will explain the four steps of those controls from WWII to the forthcoming years. The fourth section will summarize the consequences that we can draw from this information and will present what we can expect in the future. The fifth section concludes the paper by offering final thoughts, observations, implications, and analysis.

The Four Key Players

Three players have led the different existing controls since the mid-40s. But the rules of this game have been fixed by the United States from the early beginning. Since the late 90s, the landscape has changed—as a noticeable singularity of history—with the emergence of the hacker phenomenon. This fourth player, which can be considered as a real protest troublemaker that nobody really expected, entered the game with the will—and especially the technical ability—to upset the delicate balance in place, based on the principle that power is, according to Frank Herbert, "energy that learns" (1965).

The Western nation states

More than any other conflict, World War II was a war of technology (electronics, chemistry, nuclear science, radio communications, etc.) especially in the field of information. The failure in controlling the export of equipment sales and the dramatic consequences in the conduct of the war until 1942 (when the first successful cryptanalysis of the Enigma was possible) (Kahn 1996) have sensitized the U.S. and Western countries to the need for export control and dissemination of sensitive technologies or dual-use technologies, especially against the new threat posed by the communist bloc. A number of treaties and controls, similar to real selective embargoes, were put in place. Since the late 40s, these controls have taken different forms and have been diversified with the development of society, and of economic and geostrategic balances and business practices. But they are still present today and the future will just see the achievement of a program which has been planned long before.

These control mechanisms are based on an increased capacity in the field of theoretical and applied research (R&D) in order to have a substantial advance regarding science and technology, whose purpose was to anticipate and orient the direction of future controls. This research is heavily subsidized for years. These research entities publish very little, sometimes declassify in time, revealing a systematic and substantial advance compared to the academic research. Finally, their role is also to control the industrial and academic research, to fund them, to guide and to influence them as well as most of standardization bodies.

Industry

Industry (manufacturers, publishers, service companies) are in fact subject to the law of their country or international laws that are ratified nationally. This applies in particular to sensitive technologies in the case of technology export. In fact, the industry merely implements and sells technical choices that follow (real or *de facto*) national or international standards.

According to Bernard Carayon, a former French MP in charge of economic intelligence issues, "The power of a country lies in the ability to impose standards" (2003).

In the case of cryptography, the technology of block cipher encryption consists of mixing the plaintext and the secret key so that the links between the two become inextricable enough to prevent the cryptanalysts from accessing the plaintext. The problem is that the intractability also exists for those who want to analyze the security of the process. No evidence of reliable or proven security to date has been ever published; and, worse, their combinatorial richness and complexity can easily conceal backdoors mathematics. Under the influence of the USA, these systems have supplanted the other encryption techniques. They are found everywhere nowadays (computers, networks, banking, smart cards, etc.), and the statistical processes for the evaluation of the quality of randomness (U.S. Dept. of Commerce 2001a) are among the best examples. Government entities in charge of the upstream control in key countries (that is, G-20 countries) work in complete synergy with the industry, which somehow acts as the armored arm of the controls (especially for export). However, the globalization of the IT industry and its concentration in a few non-national actors only mean that control is no longer possible by most of the nation states which must deal with the offer imposed by the very few dominant nation states (government and its industry). And all clients of those actors—individuals and their own nation state—are *de facto* foreign customers of those dominant powers and, thus, subject to certain considerations regarding the export of technology. This offer is also largely funded at the level of R&D by the governments of these dominant powers.

Beyond this relationship between governments and industry are other factors and means of control. These include the weaknesses of implementation (backdoors disguised as programming or implementation flaws since the incompetence of developers can always be invoked to conceal malicious intent) promoted by the organization of unbridled commercial competition, the absence of an obligation from the governments to enforce secure development processes, the existence of undocumented features allowing backdoors, the extreme variability of versions, and a global cycle of evolution of systems requiring the user to run behind a commercial movement that places him *de facto* in a context of uncontrollable security. We have also to consider issues regarding intellectual property that protect against reverse engineering, most of the black boxes we buy. In other words, it is prohibited to analyze the products we buy or even to watch inside them.

An efficient and powerful backdoor does not summarize to a single piece of code: it is the combination of different factors (technical, organizational, human, etc.) which are known to be realized with a very high probability.

The academic community

The academic world is the third level of control. It is often used as scientific backing and, therefore, as a smokescreen. Why? Because in the field of security of information systems, most underlying problems are so complex (in the computational sense of term) that any operational advance and any evidence of security are impossible to produce. The number of internal states of a cryptographic system, for example, is greater than the number of particles in the universe (according to the closed model). It is, therefore, impossible at least to store and explore any real system. The proof of security that the academic world is trying to provide is in fact out of reach. We have reached a point where the failure to provide proof of insecurity has become a security proof in itself. Under these conditions, proving the existence of a backdoor (particularly a mathematical backdoor, that is to say, at the conceptual level) is like

looking for a needle in a million haystacks. Only the one who has put this backdoor knows where to find it and then how to exploit it.

This control is exercised in a number of ways:

- through the promotion and organization of scientific orthodoxy (coring and controlling program committees of international conferences, thematic orientation towards fashion research topics that are more likely to be published, subtle but perverse exploitation of the 'publish or perish' syndrome);
- through the control by money (state funding but also by manufacturers who are able to define and influence academics as to what fashion research topics and thematics are, see above) and by research funds and grants (National Science Foundation [NSF], National Security Agency [NSA], Seventh EU Framework Program [FP7]);

through the control by law: patents, intellectual property, scientific research themes that are potentially contrary to the law and the national security (for example, France's Article 323 of the Penal Code).The best example of this control relates to the mathematical problem of factoring (the integer-factoring problem—to split integers into a product of prime integers; a prime integer p is divisible by 1 and p only—is at the heart of most security systems. Solving this problem for large integers would put the security of all systems whose security is based on factoring difficulty or on related, into question). An easy method of factorization (still unknown at this time, or unpublished if it exists) would be prohibited from publication because of the huge implications for the security of all systems in the world. All the security of those systems would collapse causing global chaos. Such a discovery would be quickly identified at the stage of its premises thanks to the various control in place (the first one being the many internal evaluations of research) and banned from publication.

The scientific community is anything but independent. Although it can be a force for scientific proposals (and often admittedly brilliantly) it is in fact the standards (enforced at the international or national level, mainly by the United States, the latter monopolizing the standardization bodies and entities), the nation states and the industry which lead and control the game This is the reason why, despite an academic wealth in the field of cryptographic algorithms, we undergo an actual hegemony of block cipher systems and in particular of the U.S. algorithm AES-256 (U.S. Dept. of Commerce 2001a): a single algorithm to tie us all. This result has been obtained by combining political and industrial lobbying and industrial, strategic influence, threat of economic retaliations, exploitation of the fear of non-interoperability with the dominant technological power. And the academic community has just served as scientific caution or has sold his soul for some publications and honors.

The rise of the hacker phenomenon

The State/Industrial/Academic triptych worked well until very recently: the nation states choose and control which technology can be proposed to citizens; the industrial manufacturers or software vendors build and market approved products while the academic community brings a semblance of academic scientific backing. But since the late 90s, the hacker community has risen and has put everything upside down, such as a real singularity of technological history. Hackers—unlike academics—favor the results over the methods. Academic and hackers are at both ends of the activity of scientific and technical research as explained by René Thom, an eminent mathematician and philosopher of science: "Nature is such that understanding and action are not synonymous" (1991). For the academic community, the fact that techniques and results works in practice is not valid until it does not work in theory! For the hacker, it is the law of the efficiency and operational realism which must rule science and technology.

The problem is that hackers find backdoors very quickly (unless they are of a mathematical nature) even when they are hidden at the silicon level (Nohl & Starbug 2009). Because they are innovative, creative, free from conceptual straightjacket, for them no subject is dangerous or threatens their careers and image. Everything is happening now in hacking conferences (Black Hat, CCC, Defcon, Brucon, Hack.lu, Syscan, HIP, etc.). And in a society where ultra-computerized technology grinds and crushes citizens more and more instead of freeing them, hackers stand as resistance fighters and whistleblowers in an economic and strategic warfare that is increasingly evident.

A simple but illustrative case

In order to illustrate the way things are currently managed, take the example of encryption systems. Looking at the Wassenaar Arrangement dual-use list, category 5, part 2 (Information security), on page 3, paragraph 5.A.2.a.1.a, verifies that "symmetric algorithm employing a key length in excess of 56 bits" is encryption technology under control. As far as the AES (whose secret key has entropy ranging from 128 to 256 bits) is concerned, the publication of the AES is a clear violation of the Wassenaar Arrangement as well as of the different national regulations of G-8 countries that have been derived from this international arrangement.

The Four Phases of Controls History

The 'prehistory': from 1942 to 1975

The control of sensitive or dual-use technology seemed obvious from the beginning of the Second World War. The technological advance was THE most critical dimension of that era. Any technical advance was a strategic advantage indeed on both sides. At the end of the war, Western countries under the influence (or pressure) of the United States signed in Paris in 1949, the *Coordinating Committee for Multilateral Export Controls* (CoCom) (CoCom 1949) whose role was initially to prevent countries under influence of the communist bloc (USSR and China) to purchase goods, materials, and technologies that would really or potentially represent a military, strategic or economic interest. This included, for example, computers, software, sophisticated equipment for telephone, GPS technology, technology of chemistry, physics (electronics), etc. If the context of the Cold War could explain such a control at that time, it is more difficult to accept when it was enforced by the United States against European countries such as France. An example of this is found in the market of supercomputers that has long been closed to Europe and has started to open up at the dawn of the 90s.

It is interesting in this context to consider an unprecedented event that occurred in 1977: the publication, for the first time ever, of a ciphering algorithm, the DES (*Data Encryption Standard*) (Fips Pub 46 1977), by the U.S. government with technical support of the NSA. This algorithm was presented as a highly secure one. This analogy should make the significance of this event clear to readers: publishing such know-how in the field of highly secure communications would have been equivalent to publishing the plans for the nuclear weapon (H-Bomb).

Who can believe seriously that such a publication in the CoCom context was possible without any form of control upstream? This publication would otherwise have constituted a serious violation of the CoCom. In fact, later in 1992 the publication of certain works of researchers (Biham & Shamir 1990) and the corresponding embarrassed response from the NSA have provided hindsight regarding this issue. NSA acknowledged, more or less explicitly, that it

began to work on DES-like technology since 1966 at least, although its official birth was in 1975. The control probably lies at mathematical backdoors level. Note that so far, it is still impossible to investigate and explore computationally DES exhaustively and, therefore, find these backdoors.

Finally, the publication of this algorithm gave birth to an actual academic community in cryptology. This community was indeed *de facto* strongly influenced, therefore, 'directed and oriented' by mathematical concepts of U.S. and government origin; nobody has been able so far to prove the actual security, due to the huge combinatorial complexity, of these concepts. The 'proof' of security for these algorithms, which can be seen as a 'default' proof, lies, in fact, in the inability of the academic community to produce a single operational attack.

This publication has given rise naturally to all other ciphers marred with the same conceptual backdoors, thus making them automatically controllable: for example, the IDEA algorithm (directly inspired by the same mathematical concepts in DES), which is included in the common user-oriented encryption software PGP. The PGP case was at the heart of what must be considered a "true-false" or fake legal case designed to encourage people to use alternative software, however still under control, and hence to manage a growing mistrust *vis-à-vis* the DES. Philip Zimmermann was probably sincere and convinced of the security of PGP, and he was himself the victim of a subtle control technology policy, prepared years ahead.

It is important to remember that, unlike almost all countries and transnational organizations (approximately 120 in 1995), General de Gaulle made it mandatory, for any nation state (military, diplomatic, economic, political) needs regarding communication security and encryption means, that France use national equipment designed (from the mathematical concepts to the very final implementation) and built by national entities only. (The reintegration of France into the integrated NATO command raises 'questions' from a few of the decision makers on the need to maintain such a French specificity. To maintain full interoperability with NATO, why not adopt the tools of our 'American friend' and, therefore, reduce costs in this area. It illustrates that culture and sociology may be another control tool.) In 1995, the Hans Buehler case (Strehle 1994; Filiol & Richard 2006) showed that all the countries that had not done so, had seen their encrypted communications heard by the U.S. for over 50 years, thanks to mathematical and implementation backdoors put in all enciphering devices that had been sold to those countries. It proved, once again, the extremely clever vision of General.

The transition phase: from 1975 to 2001

The birth of a scientific community in the field of information and system security as well as the evolution of society itself (especially with the spread of computer and networks for all citizens, the fall of Eastern bloc in 1989, and the various geopolitical upheavals) made, from the late 70s, the CoCom type controls difficult to explain, maintain, and manage. The period 1977 to 2001 was marked by the end of the Cold War, the rise of terrorism, and the beginning of the global economic war that no longer hides its name. It became, therefore, necessary to diversify the controls according to the principle of eggs and basket.

CoCom was dissolved in March 1994, and quickly replaced by the Wassenaar Arrangement (Wassenaar 1996), which defines twelve lists of materials and technologies subject to controls (42 countries have signed this agreement up to now). Other controls, less visible, however very efficient, are also taking place: the Socrates project, GATT, and later WTO with the aim

of building a global world economy (see next step) to organize and lead the technology standardization under U.S. influence (particularly regarding technology related to the Internet), the mutation of national laws and regulations (supranational laws [European treaties or laws] become automatically national laws), and the development of monitoring networks like Echelon. So the world is changing, and the controls are organized and adapted to follow those mutations. The target is no longer a few communist states, but every citizen of the world, equipped with a computer who is both a potential consumer in a world under globalization and/or a potential terrorist (Islamic, anti-globalization, occupy Wall street, Anonymous, etc.). The 'threat' becomes diffuse, polymorphic, so fine in granularity that it is necessary to globalize controls and their management.

The globalization phase: from 2001 to 2012

With the rise of terrorism, the 9/11 attacks on the one hand and the alter-globalization on the other hand, another dimension has emerged: that of emerging countries (China, India, Gulf countries, etc.), which most often have not signed the Wassenaar Arrangement. The control of technology that is spreading everywhere must become a control set up well in advance. It is necessary to globalize in order to concentrate technology and its marketing in the hands of a very few multinationals that are easier to control. To reach that goal, from 2001 to 2012 many news control levels have been implemented:

- The dominance of the private sphere over the public sphere. Nation states can no longer close their market: they are open to competition (WTO effect under U.S. influence while the latter are closing their own market). It is the political level of controls. The aim is to weaken the current political landscape, consisting of nation states exercising their economic and political power and hence still owning pieces of sovereignty.
- Take-over bids, M&A (Mergers and Acquisitions), elimination of competitors, concentration of production and services (that is, the market of routers with Cisco versus Huawei). Here lies the economic control: the free competition imposed by the WTO and the subsequent various deregulations (with a U.S. protectionism which becomes even stronger in parallel) have shattered the last control capabilities at national level by the gradual disappearance of national technology champions.

Without loss of generality, one example will suffice to illustrate this phase: the liberalization of cryptography. It was initiated in 1997 with the Hourtin speech of Prime Minister Lionel Jospin under the pressure from the U.S.A. and has, in fact, led to the hegemony of a single cryptographic algorithm: the *Advanced Encryption Standard* (AES) (U.S. Dept. of Commerce 2001a), which, once again, has been offered to the world for free and openly, by the U.S. Department of Commerce, with the technical assistance of the NSA. Readers should recall that the official publication of the algorithm occurred in a rather critical context: the rise of terrorism, of rogue states such as Iran and North Korea. This would mean a direct and clear violation of the Wassenaar Arrangement and of any embargo in place at that time! Anyone who uses this algorithm *de facto* protects its communications and data against eavesdropping (naïve view) or falls under the control of the one who knows the backdoors in place (realistic view).

It is possible to give many other examples: RIM/Blackberry, the microprocessor industry (the disappearance of AMD, Sun, powerpc, RISC processors in favor of Intel products only), operating systems, and Facebook/Google/Twitter which results in the mass surveillance of at least one billion people.

In 2012, a massively computerized, networked society was finally obtained, one which enables the spread of thousands of backdoors of very different types: 0-day vulnerabilities relentlessly renewed day after days, sophisticated state malware (as spying malware like Magic Lantern (USA), Bundestrojan (Germany), Stuxnet, etc.). In short, this world makes the Orwellian vision a simple fairy tale or a children's story.

The 'Legal' phase: from 2013 to…

What will follow next? This whole edifice cannot stand and be viable without a final dimension: the dimension of law. Beginning in and moving forward from 2012, the world is witnessing the rise of supremacy of laws over the international business, in primarily two main dimensions:

- Intellectual property regulations. Multinationals' place, power, interest, and influence must be protected. PIPA/SOPA/ACTA, software patents, patent wars (for instance, Samsung vs. Apple, but previously NOVELL vs. France Telecom), and a standards war are only the beginnings of this trend.
- The rise of laws related to cyber defense and the demonization of actors who stay beyond the existing controls (such as hackers, for example with Vupen or CoseInc cases): the extension of the geographical territoriality to the digital territoriality (of a computer server within a U.S. domain name, even located outside the U.S., is considered as a part of the U.S. territory), the Patriot Act and its various variations from Bush to Obama, cybercrime laws.

Consequences and Discussion

In the end, all of the above has led to the concentration of technology and services in the hands of a very few states and multinationals that have absorbed and/or eliminated competition. They are now in control of everything, putting the rest of the world in an obvious dependency state that must be the ultimate control. In the growing context of cyber warfare (defensive but also offensive), this economic domination in fact hides the strategic dominance (both at political and military levels). The confrontation of Cisco vs. Huawei should not be considered (except by the naïve) as a mere technological and economic confrontation. This is the strategic dominance of the information passing through their routers—accessible via the backdoor they can hide inside. This is the real dimension. It is the same for many other cases: Samsung/Apple, Microsoft /Android/Linux. In this context, the Intel/Microsoft agreement around UEFI technology (with the consequence of binding equipment [computer] to a unique operating system thus preventing the installation of any other alternative system) is a clearly worrying and terrifying trend.

In this gigantic worldwide game, it seems that China and other emerging countries (for instance, South Korea, India, Brazil, and the Gulf States) are poised to put sixty years of U.S. hegemony, and, by extension, Western countries influence, into question. From the Monroe Doctrine (however revised by the U.S. intelligence at the end of the Second World War) to the Chinese vision of globalized confrontation as defined in the book "Unrestricted Warfare" (Qiao & Wang 1999), it appears that the world could experience a change of game and switch from the game of chess to the game of Go.

The rapid economic development of emerging countries which have not signed the Wassenaar arrangement should, therefore, be considered under a new light. Those countries have been

the victims of this arrangement for over fifty years. It is very likely that they will choose to take their revenge and consequently not to ratify the Wassenaar arrangement. As with China, the growing economic dominance could become a strategic dominance. It is not sure whether the declining influence of the U.S. is still strong enough to impose controls as it was, for example, regarding the laser printers in 2001. (The *Electronic Frontier Foundation* in 2001 revealed that most laser printers marked printed material with micro-points. From any printed page, it is possible to trace back to the printer and then to its owner).

Conclusion

In addition to the results mentioned in this paper, the evolution of these controls has a direct impact on innovation in Western countries; and the medium to short term, those countries may become nations of second order. In fact, for the innovator, it is wiser to create a company in a non-Wassenaar country.

It is, therefore, essential to quickly restore the capacity and willingness of national sovereignty or at least in Europe in the area of sensitive technologies, driven by SMEs/SMIs. If Wassenaar-like controls are undoubtedly necessary to protect the safety and interests of the state and its citizens, the latter must receive assurances from their governments that control is strictly enforced by their governments only, not by outside actors (another state [such as the U.S.A. or China], multinational companies, etc.)

In other words, citizens should still have the choice of the backdoor, if there should be. Backdoors are not inevitable. It is possible to provide truly secure tools (as are national versions of the technology when they still exist) without backdoors. The needs of a sovereign country can be assured more at the national level by law and through the respect of citizens for their nation state. The problem is not technology, but the power and the consideration that each citizen gives the state.

It is necessary—even vital—to have a truly independent and active academic community which is still the master of its own destiny and not subject to the dictates of the Shanghai ranking (another form of control where the size outweighs the quality).

References

Biham, E & Shamir, A 1990, *Differential cryptanalysis of DES-like cryptosystems*, Advances in cryptology CRYPTO 1990, Lecture Notes in Computer Science, Springer Verlag, Heidelberg, pp. 2-21.

Carayon, B 2003, *Intelligence économique, compétitivité et cohésion sociale*, France National Assembly Report, viewed October 2012, <http://www.ladocumentationfrancaise.fr/rapports-publics/034000484/index.shtml>.

CoCom Archives, 1949–1994, viewed October 2012, <http://www.diplomatie.gouv.fr/fr/ministere_817/archives-patrimoine_3512/fonds-collections_5143/organismes-internationaux_11594/cocom-1949-1994_25985.html>.

Electronic Frontier Foundation 2001, viewed October 2012, <https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots>.

Filiol, E & Richard, P 2006, *Cybercriminalité – Les mafias envahissent le web*, Dunod, Paris, viewed October 2012, available under Creative Common License on <https://docs.google.com/viewer?a=v&pid=explorer&chrome=true&srcid=0B6BlkqAoxXq1ZDIzZDVjY2QtMjZjNi00NTNmLTkzNmItMDQ4NDc5YWYwYjdk&hl=en_US>.

Herbert, F. 1965, *Dune*, Chilton Book Co Publishing, New York.

Kahn, D 1996. *The codebreakers - the comprehensive history of secret communication from ancient times to the internet*, Macmillan Publishing, New York.

Menezes, AJ, van Oorschot, PC & Vanstone, SA 2001, *Handbook of applied cryptography*, CRC Press, New York.

Nohl, K & Starbug 2009, *Silicon Chips: No More Secrets*, PacSec 2009, Tokyo, viewed October 2012, <http://www.degate.org/Pacsec2009/091001.Pacsec.Silicon.pdf>.

Qiao, L & Wang X 1999, *Unrestricted warfare*, People's Liberation Army, Literature and Arts Publishing House, Beijing, viewed October 2012, <http://www.terrorism.com/documents/TRC-Analysis/unrestricted.pdf>.

Strehle R 1994, *Verschluesselt – Der Fall Hans Buehler*, Werd Verlag, Zurich.

Thom, R. 1991, *Comprendre n'est pas expliquer – Entretiens avec Emile Noel*. Flammarion, Paris.

U.S. Dept. of Commerce/National Institute of Standards and Technology 2001a, *Advanced Encryption Standard*, FIPS PUB 197, NIST, Gaithersburg, MD, viewed October 2012 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

U.S. Department of Commerce/National Institute of Standards and Technology 1977, *Data encryption standard (DES)*, FIPS PUB 46, NIST, Gaithersburg, MD.

U.S. Dept. of Commerce/National Institute of Standards and Technology 2001b, *Security requirements for cryptographic modules*, FIPS PUB 140-2, NIST, Gaithersburg, MD, viewed October 2012, <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

Wassenaar Arrangement 1996, viewed October 2012, <http://www.wassenaar.org>.