Cryptology, Digital Assassination and the Terrorism Futures Markets

R. Sukumaran

Abstract

A recent news item indicated that the US Government had been planning a website that would enable people to place bets on the likelihood of terrorist events. It was hoped that a study of market trends would enable intelligence agencies to anticipate and prevent such events.

The idea was mooted by Admiral John Poindexter, head of the Total Information Awareness Program and bears some resemblance to a scheme mooted by Jim Bell. Bell, an MIT graduate had proposed a scheme which uses cryptography and the Internet in order to eliminate corrupt public officials. His scheme rewards those who correctly predict the date of death of such officials. However, the identities of the successful predictors were to be kept secret by using public key encryption methods. Bell claims that his scheme, if universally adopted, would lead to the elimination of government itself. Society would regulate itself by the threat of assassination of those acting inimical to its interests. No other regulatory mechanism, he claims, would be required.

This paper attempts to understand Jim Bell's concept which requires some knowledge of cryptology. It briefly discusses some concepts in cryptology and electronic banking which are essential to the working of the scheme. It also discusses the Iowa Electronic Markets which have been fairly successful in predicting US Presidential elections. It uses an approach similar to that proposed by Admiral Poindexter's group. The paper analyses the practicality of both Bell's and Poindexter's schemes.

— * —

Introduction

In late July 2003, the US media was rocked by news that the Pentagon was planning to open a website that would enable investors to place bets on the probability that a particular event — a terrorist attack or assassination — would

Strategic Analysis, Vol. 28, No.2, Apr-Jun 2004
Revised paper received on May 8, 2004

take place.[1] The programme, called the Futures Market Applied to Prediction (FutureMAP), was part of the Total Information Awareness Program and was coordinated by the Defence Advanced Research Projects Agency (DARPA). The key figure in the plan was retired Admiral John Poindexter, a prominent actor in the Iran-Contra scandal that bedevilled the Reagan administration. Its purported aim was "to explore new ways to help analysts predict and thereby prevent the use of futures market mechanisms."[2]

The terrorism futures market bears a certain resemblance to a scheme called 'Assassination Politics', propounded by Jim Bell, a disgruntled American cyberpunk and MIT graduate.[3] Jim Bell has used the ideas of cryptography and e-banking to develop a concept he calls 'Assassination Politics' or 'DigitaLiberty'. He conceives of an organisation that would assist in eliminating corrupt officials and oppressive politicians through a system of rewarding those who correctly predict the date on which a particular official or leader will die. The identities of the successful predictors would be kept secret using encryption. Bell believed that the successful implementation of his system would result in the eventual abolition of all forms of state control and even war.

Interestingly, Jim Bell was imprisoned in 1997 for threatening a US federal agent following the publication of his scheme. This, coupled with his refusal to pay tax demands he considers illegal, brought down on him the wrath of the Internal Revenue Service (the American equivalent of the Income Tax Department).[4] The apparent co-option of his scheme by the Pentagon therefore deserves closer scrutiny.

The Basics of Cryptology

Codes, Ciphers and Frequency Analysis

In order to understand Bell's system, we digress a little into cryptology — "the science of rendering signals secure and extracting information from them."[5] This comprises both cryptography — "rendering information unintelligible to outsiders by various transformations of the alphabet", and cryptanalysis — the method of breaking down or extracting the message from the intercepted signal.[6]

Technically, substitution at the word level is known as encoding.[7] Thus, if we replace 'I am here' by '1 2 3', where 1 represents 'I', 2 represents 'am' and 3 represents 'here', we would have encoded the message. Substitution at letter level is *enciphering*. This can be done by *transposition*, where the letters constituting the message are re-arranged, thus forming an anagram or by *substitution* in which each letter of the alphabet is replaced by another according to a certain pattern.[8] If we replaced each letter of a message by another in a certain pattern, we would have enciphered it. Many encryption schemes use a combination of transposition and substitution incorporated in a specific pattern, controlled by a *key*.[9]

Encoding messages requires a code-book, which contains an equivalent for every possible word that could be used.[10] It would therefore be a fairly hefty tome. Every person in the transmission-reception chain would need a copy. The loss or capture of a code-book would be catastrophic and preparing and distributing a replacement would be a nightmare. Around the 16th century, codes were therefore replaced by ciphers. Ciphers need to cater only for the limited number of letters in the alphabet, instead of for the entire lexicon of words.[11]

Around the 8th century, the Arabs discovered that some letters of the alphabet occur more often than others in any message.[12] They also found that the frequency of the occurrence of these letters is independent of the message, provided it is long enough. In English, the letter ‘E’ occurs most often, followed by ‘T’ and ‘I’. the Arabs were possibly the first to use frequency analysis to decipher messages, without knowing the ‘key’.

Mono and Poly-Alphabetic Ciphers

The simplest form of substitution ciphers are called *Caesar ciphers* after Julius Caesar who is believed to have used them.[13] These involve replacing each letter in the message by another a fixed number of places away in the alphabet (called a Caesar shift). If ‘a’, ‘b’ and ‘c’ were replaced by ‘d’, ‘e’ and ‘f’ respectively, we would be using a Caesar shift of three. The English alphabet permits Caesar shifts of up to 25. The alphabet re-arranged according to the Caesar shift is called the cipher alphabet. However, we need not stick to simple Caesar shifting. We could also rearrange the letters of the alphabet randomly to form different cipher alphabets. This would give rise to an enormous number of permutations making deciphering much more difficult.

Simple and even random substitution ciphers are however vulnerable to frequency analysis. This led to the development of poly-alphabetic ciphers.[14] Here, each letter of the message is enciphered using a different cipher alphabet.[15] This is determined by the keyword chosen. Depending on its location in the message and the length of the keyword, the same letter could be enciphered differently. This form of encryption, known as poly-alphabetic encryption, is immune to normal frequency analysis. While the enciphering technique might be common knowledge, how the process works depends on the keyword.

The Importance of the Keyword

The 16th century de Vigenere cipher was poly-alphabetic. This meant that the cipher changed with every letter of the message. The pattern was decided by the keyword. Keeping the keyword secret therefore became the cryptographic problem. It had to be agreed beforehand by both parties. The keyword decides which particular cipher alphabet of the de Vigenere Table will be used to encrypt each letter. The encrypted message thus contains as many cipher alphabets as the number of non-repeating letters in the keyword. The longer the keyword, the more secure the cipher. The receiver uses the keyword again to decipher the message. The de Vigenere cipher was considered to be practically unbreakable for the next four hundred years since it was invulnerable to simple frequency analysis.[16] When it was eventually broken by Charles Babbage and Friedrich Kasiski in the 19th century, deciphering was made possible because of restrictions imposed by the keyword selected.[17] One possible solution was not to use meaningful words as keywords. Another was to use keywords as long as the message itself. However, there still remained the problem of informing the receiver what the keyword was.

Many different approaches were used to provide strong encryption. The German Enigma enciphering machine designed by Arthur Scherbius and patented in 1918, used poly-alphabetic ciphering. The Enigma used three scramblers, which meant that every letter went through three stages of substitution. Interchanging the scramblers further increased the number of possible scrambler arrangements. It also had a plugboard, which interchanged six pairs of letters (transposition).[18] The total number of arrangements possible on the Enigma was a staggering ten million billion (10^{15}).[19] Despite all its features, the Enigma encipherment was eventually broken because it used a key for setting the scrambler positions.

Solving the Key Distribution Problem: The Advent of Public Key Cryptography

The main problem the sender and receiver had was that of agreeing on a key. If the key were intercepted, the message could be read. The problem of how to agree on a common key, without an eavesdropper being able to intercept the key, is known as the key distribution problem.[20]

In 1976, Whitfield Diffie and Martin Hellman of Stanford University, proposed a solution to the key distribution problem involving the use of one-way mathematical functions. When a number is input, these functions produce a unique output. However, the process is not reversible. Two persons, A and B, use a one-way function of the form y^x (modp).[21] They agree on values for y and p over an open line, but choose values for x that they keep secret. Both now insert their values for x into the one-way function and exchange their results. These values are inserted in place of y in the one-way function and the result again calculated. The results are identical. This becomes the key and it can be used to operate a symmetrical cipher. A and B have therefore managed to agree, without meeting, on a common key which they can use for enciphering and deciphering messages. To take a simple example, an eavesdropper would know that A and B have agreed to use the values y=7 and p=11, in the function y^x (modp), but would be unable to work out their respective values of x. The values of y and p actually used are very large, thus making life more difficult for any eavesdropper.

Asymmetric Keys

Thus far, all keys had been symmetric — the same key being used for both enciphering and deciphering. Whitfield Diffie therefore visualised a system which would use an asymmetric key. One key, widely publicised, would be used for enciphering and another key, solely in the possession of the receiver, would be used to decipher the message. However, Diffie did not have an example of a function that could work in the manner he envisaged. The problem was solved in 1977 by Rivest, Shamir and Adelman, who evolved what is now called the RSA system, after their initials.

Public Key Cryptography — the RSA System

Rivest, Shamir and Adelman used a one-way function. One-way functions are non-reversible. Just by knowing the function used and the output obtained, one cannot work backwards to obtain the input. Rivest and his colleagues used a one-way function based on modular arithmetic. The message is digitised and put into the function which generates another number called the ciphertext. The system essentially uses the fact that it is exceedingly difficult to factor the product (N) of two very large primes. N is called the public key.[22] To send a message to A, B inserts her public key and the message into the one-way function and sends the result to A. Merely knowing A's public key is not enough for anyone to decipher the message. He also requires A's *private key*. The private key is related to the primes that A multiplies together to obtain the public key. However, it is difficult to factorise a very large number into the two large primes that are its factors. If the prime numbers used are of the order of 10^{65}**,** the number N would be of the order of 10^{130}. Factorising such a number could take a 1 GHz Pentium with 128 MB of RAM several months. Actually, the values of N used in important transactions tend to be much higher.

Hash Functions and Digital Signatures

Digital signatures were originally suggested by Diffie and Hellman as a method of verifying that a message had not been tampered with and that it had indeed been sent by the purported author.[23] These are generated using hash functions. A hash function H takes the message m and transforms it into a sequence of fixed length, whatever the size of the original message. This is called the hash value h (i.e., h = H(m)). Reversing the process should not yield the message m or its length. Hash functions employed in cryptography are usually chosen to be collision-free, i.e., no two messages will result in the same hash value. Further, neither the message nor its length can be extracted from the hash value. A first encrypts a message using B's public key and sends it to him. B uses his private key to read the message. In order to generate a digital signature, A inputs her message into a hash function. She then encrypts the resulting hash value using her private key and sends the result to B separately. B extracts the hash value using A's public key. He then applies A's hash function to the original message. If the resulting hash value is the same, it proves that the message has not been tampered with and that it was genuinely originated by A.

Privacy and e-Banking

Digital Cash

Personal privacy is now a major public concern. Increased computerisation has resulted in credit card companies and banks creating huge databases on customer preferences and spending patterns. Despite assertions to the contrary, this information is often sold to other commercial interests and can also be linked to virtually build up a dossier on any particular individual. This information can be misused by various agencies, including the government.

Increased computerisation has resulted in the development of digital cash. These are essentially numbers which represent a certain sum of money. A bank would sign (superimpose) a particular series of notes with its digital signature (private key).[24] All notes signed with this particular key would have a certain value. These bank notes could be authenticated using the bank's public key. Thus, if A wishes to withdraw a dollar from her bank, she first generates a random number, signs it with her private key and sends it to the bank. The bank verifies her signature with the public key she has earlier agreed for transactions with the bank. It then removes her signature, signs the number with its own private key, certifying that it is worth one dollar and returns the now valid note after debiting her account by one dollar. This note can now be used by A to pay for goods in B's shop. B can verify the note by checking the bank's digital signature. He then sends the note to the bank. The bank verifies its own signature and the note number and notes that it has been spent by A. It then credits B's account with one dollar, simultaneously debiting A's account by the same amount. The note cannot now be double-spent. However, the system described does not have privacy since the electronic notes can be tracked.

Blind Signatures and Digital Pseudonyms

In a paper published in the *Scientific American* in August 1992, David Chaum and his colleagues outlined a scheme to prevent such digital cash being traced. They developed a system they called 'blind signatures'.[25] When sending a note to the bank, its number is multiplied by a random factor. The bank therefore does not know its number. It only knows that A has sent it. Once the bank has signed and returned it, A removes the blinding factor. Since the bank has no knowledge of the actual note number, transactions cannot be linked. The notes cannot be traced since the blinding factor is unknown.

In the same article, David Chaum also described a concept called a 'digital pseudonym' which would ensure privacy while at the same time-enabling a person's identity to be validated. A person could choose different digital pseudonyms for every organisation that he/she does business with. This would be done by using 'electronic representatives' and 'electronic observers'.[26]

An electronic representative would reside on a smart card with a keypad and display. It would control all electronic transactions that its owner makes, all data input and generate the private and public keys required for a transaction. This would ensure total privacy and untraceability of transactions.

'Electronic observers' would prevent double-spending of digital banknotes and protect the interests of banks. The observer would reside on the smart card along with the electronic representative and monitor its behaviour. Observer and representative would be programmed not to trust each other. In order to protect its owner's interests, the representative would be in overall control and ensure that unauthorised transactions are not carried out. Observers would be validated by validating authorities. These would also authenticate the various digital pseudonyms that a person requires for transactions with different agencies. The validating process would assure any agency transacting business that a genuine person exists behind the digital pseudonym.

Assassination Politics or DigitaLiberty

An American anarchist named Jim Bell has integrated all these aspects, into a system for the elimination of corrupt Government officials.[27] Jim Bell is an MIT graduate, presently serving a term in prison for threatening a US federal agent. His original grouse seems to have been that he was unfairly taxed. His scheme, which he calls DigitaLiberty, has been published on the Internet under the title "Assassination Politics".[28] The effectiveness of Jim Bell's scheme hinges on the concept of digital cash and digital pseudonyms, as envisaged by David Chaum and on securing personal anonymity through the use of Public Key Cryptography (PKC). It envisages an organisation which would act as a combination of bulletin board, mail forwarder and lottery manager. It would maintain a list of particularly disliked public officials and separate accounts for each person. The organisation would also display details of the money that it has received as contributions from the public in each account. This amount would be paid to the person who successfully predicts the date of that individual's death.

An individual would send to this agency, an encrypted envelope containing some digital cash encrypted with the organisation's public key. Inside this envelope would be another, containing his prediction for the date on which a particular official would die. The second envelope is encrypted using the person's private key and hence cannot be opened. The organisation would open the first envelope with its private key and discover the digital cash. It would not, however, be able to open the second envelope without the public key which the predictor retains. It thus does not know whose death has been predicted and when. People aggrieved by an individual could also send the organisation some digital cash to be paid to the person who correctly predicts that individual's death. When the prediction is proved right, the predictor wins the reward which has been posted, for anyone who correctly predicts the death of that individual. Bell suggested that the use of (PKC) and digital pseudonyms would ensure absolute anonymity. This would prevent people being targeted for criminal activity by government agencies like the

FBI. In any case, no one would be carrying out any illegal activity because people would merely be predicting the dates on which some particular individuals would die. No one would be incited to carry out a killing. The reward would be due whether the person died a natural or unnatural death.

Preventing Frivolous Predictions

In Bell's system, the name of the official and the date of his predicted death are both encrypted using PKC and cannot be read. The prediction would be posted on the bulletin board. In order to ensure that frivolous predictions are not sent in, individuals would also have to enclose some digital money. This money would be added to the amount sent in by all those who have also predicted or wish the death of that particular individual. There would be nothing to indicate the identity of the person sending the prediction. The amounts contributed for the death of a particular person would be publicly posted on the bulletin board.

Protecting Identity

If the prediction comes true, the person who has correctly anticipated the death of the particular individual would send the organisation the key to decode his prediction. The organisation would open his envelope and discover the name and date of death correctly predicted. The individual would also send another public key which the organisation would use to encrypt the reward. The public key would be posted to enable anyone else, who wishes to do so, to send money to the successful predictor. The use of PKC, digital pseudonyms and blind signatures would ensure the anonymity of the successful predictor. Further, no one would know what role, if any, he had played in the demise of the individual. Even if it wished to, the organisation could not assist any authority which wished to trace the successful predictor. Even the digital cash would not be traceable to its source.

This is the essence of Jim Bell's system. He summarises its advantages as follows: The prediction can be made in total anonymity. Since the prediction itself is encrypted and revealed only on the death of the 'target', the target cannot be warned. The predictor need not reveal his prediction, unless he chooses to. He need not claim the reward either. He can transfer it to anyone else since it can be blinded. The organisation, too, does not know the contents of any prediction and therefore cannot be held liable for any criminal activity. However, for the system to work, a potential predictor would also have to be convinced that the money posted would actually be paid for a successful prediction.

How It Works

Assume that a citizen is upset with a government official or politician who is corrupt or violates his rights. He mails the individual's name and his predicted date of death to the organisation along with any amount of money that he considers appropriate. If even 1 per cent of the population of India were willing to contribute Rs 1/- towards the reward, the amount collected would total Rs one crore. The successful predictor could collect his money knowing that his identity is safe and not dependent on the benevolence of the organisation. The money he receives would also be untraceable to its source.[29]

Governments could target the organisation for promoting criminal activity. However, Bell argues that the organisation could not be charged with criminal activity because it is merely forwarding mail. It also could not be charged with being an accessory after the fact since it would not know what information is contained in the encrypted digital envelopes. It would not itself be engaged in any criminal activity. There would be no conspiracy because there are no co-conspirators. All participants would be anonymous. The predictions are themselves encrypted and the name of the target unknown. However, one interpretation of the law suggests that the organisation could be considered to be acting criminally in 'endeavouring to persuade' people to murder. However, Bell suggests that the organisation would, in fact, become global and therefore, difficult to target under national laws. It would then bear comparison with international terrorist networks. Further, the mere fact that no laws now exist to combat such organisations does not mean that this will always be the case. It is more than likely that specific laws would be drafted to target any group planning to enter this 'niche' business.

Revolutionising Society

Bell suggests that the implementation of his scheme would revolutionise society.[30] He goes so far as to suggest that even the police and military could be abolished. Leaders of bellicose states could be removed without the dangers of war. No leader would be immune.

In most cases, it is the general population which has the most to lose from war. The availability of such a system would ensure that countries are not pushed into unpopular wars. Bell feels that this would result in a de-bellicisation of international politics and even remove the need for large armies. He suggests that why this has not happened so far is because it has been left to the leaders themselves. Earlier, a deed could be done but the doer could not be rewarded without fear of discovery.

The perpetrator could be traced and punished by the police. The beauty of his system is that successful predictors could be rewarded without any risk of discovery. The random nature of the whole process ensures a disconnect between predictor and target.

Such a system would also ensure that no judges or prosecutors would be willing to take up any case on behalf of an unpopular government since they could also be targeted. Any dishonest organisation (one which failed to pay the promised reward for a successful prediction) which goes into this business could itself be targeted or forced out of the market by a similar, but more honest organisation. The ethics of the marketplace!

Self-Regulated Policing

Bell also suggests that crime itself would reduce. According to him, the police are generally unable to prevent serious crime and prefer to target 'victimless' crimes like pornography, prostitution or gambling. However, the cost of maintaining a police force is enormous. He suggests that a self-regulating system could be created for a fraction of this cost. He feels that people would be willing to contribute a small sum in order to predict the death of a malefactor, say a car thief. Even insurance companies would be willing to reward successful predictors, in order to reduce losses caused by payouts for car theft claims. This would result in car theft becoming a risky proposition.

Competition from Criminal Organisations

The other fear is of criminals using similar methods to set up an organisation targeting law-abiding people — a modern-day variation of extortion. However, with an unethical organisation, there is no guarantee that payment would let you off the list. Such an organisation would be willing to target anyone, not just wrong-doers.[31] The advantage of the legitimate organisation is that it would target only evil-doers. The monetary incentive for terminating evil-doers would therefore be higher than for targeting an ordinary individual in whose death hardly anyone would have any interest, The criminal organisation therefore may not continue long in business. The ethical organisation would survive.

The Viability of Digital Assassination

From cryptography to the elimination of intrusive government the police, the military and war itself, is truly a giant leap. But does this system stand up under examination? It is true that PKC, digital pseudonyms and blind signatures would enable identities to be kept secret. However, it presupposes that, given the public key, determining the private key would be difficult. PKC depends to a large extent on the huge amount of time that it takes to factorise very large numbers. However, computers continue to become smaller and faster. It is also not impossible that mathematical algorithms enabling faster factorisation of huge numbers could be developed. These could significantly reduce the time factor. However, it is equally likely that PKC would then use much larger numbers and also that different encryption methods using asymmetric keys could be developed.

The kind of scheme Bell proposes is likely to threaten established forms of government. It is unlikely that an establishment, aware of the threat such a system would pose to itself, would allow its creation. Such an organisation would need to be visible, accessible and with public support.

The technology proposed to be used is only likely to be found in advanced countries which presumably have an active citizenry concerned about governance and civil liberty. The system also assumes widespread awareness among the public of advances in cryptography and electronic banking. But people in most countries are wary of the claims advanced for new technology. Further, new technology is generally controlled by capital which already owns the technology currently in use. New technology will therefore, generally be suppressed until society has been sufficiently prepared for its introduction — the aim being to maximise profits. Thus, for example, we may be reasonably certain that the replacements for fossil fuels, as and when they arrive, will be controlled by the likes of Royal Dutch Shell and Exxon, which controlled fossil fuels in the first place.

The fact that this system requires the availability of advanced technology rules out its adoption in the developing world which would possibly benefit the most from the implementation of such a system. It is unlikely that it could work with the kind of primitive infrastructure that is available in most of the developing world. In fact, it is highly likely that it would be an attractive proposition for adoption by criminal organisations in the developing world, given the lack of activist interest in issues of governance and the difficulty of mobilising public opinion. It therefore seems that Bell's scheme will remain an interesting study in the use of technology for the abolition of intrusive government and be added to the many schemes for world government that have cropped up in the past.

Bell does not specify who will run this organisation. It will need capital, equipment and, most important of all, personnel. How will it be funded? It will obviously need to keep a percentage of the donations people send it for its own operating expenses. The key to the organisation is its personnel and their integrity, since it is they who would maintain the website and post the rewards.

The Terrorism Futures Market

In late July 2003, news broke that the Pentagon was researching a scheme called the Futures Market Applied to Prediction (FutureMAP). [32] The idea had been broached by Admiral John Poindexter, National Security Adviser to President Ronald Reagan and a prominent casualty in the Iran-Contra affair. The budget for the program was apparently US$ 8 million. The program was part of the Total Information Awareness Program and was coordinated by the Defense Advanced Research Projects Agency (DARPA).

Admiral Poindexter, who has a PhD in nuclear physics, has had a controversial career.[33] He has apparently specialised in offering unorthodox solutions to difficult problems. In the Iran-Contra affair, he and Col. Oliver North sold weapons to Iran, then under US sanctions for holding American hostages. With the proceeds, he financed the Contra insurgents to overthrow the Sandinista regime in Nicaragua.

Poindexter's latest idea is to allow investors to bet on their predictions of likely terrorist actions to help law and intelligence agencies anticipate better where the next outrage could take place. This system is supposedly modelled on the Delphi method of forecasting, pioneered by the RAND Corporation. The assumption is that, investors acting en masse, could pool their bits of information together to create a far better picture of reality than they could individually. A better picture of the future of the stock market or the national economy should thus emerge.

The Iowa Electronics Markets

This principle is already being used in the Iowa Electronics Markets to predict the outcome of presidential elections. The Iowa Electronics Markets are small-scale real money markets run by the University of Iowa Business School. The most well-known of these is the Presidential Futures Markets, which aims to predict winning candidates in the Presidential elections. Essentially, traders are asked to answer which candidate they think people would vote for on election day. A cocktail of options is offered. The system uses classical statistics, a representative sample of voters and assumes truthful responses to arrive at a prediction of the result.[34] This is done on a daily basis. Trading is frozen on the night before the election and the results compared with the actual results.

Each market is linked to a specific future event. Traders are offered a bundle of contracts, each contract relating to a particular subset of the main event, for example, the likelihood of a particular Democratic candidate winning against any Republican candidate, or a particular candidate being nominated by a particular party. Each bundle consists of one of each contract available in the market. The bundles are bought and sold by the system at a price which is the aggregate pay-off for that outcome as determined by the market. The system merely introduces contracts into the market. Traders can exchange these at prices that they decide. Traders only know the best bid and ask for prices and the last trade price. They do not know the quantities available at these prices.

Joyce Berg and her fellow researchers at the University of Iowa have discovered that the system is fairly accurate as regards US Presidential elections. Accuracy is enhanced when the event is high profile and arouses general interest by market volume. They have also discovered that markets with fewer contracts, i.e., fewer variables (candidates) are more accurate.

FutureMAP

With FutureMAP, Poindexter attempted to extrapolate the Iowa Presidential markets system to the prediction of terroristic events. Each of these outcomes would become a contract. It was assumed that the information available to various players in the market could be used to determine the likelihood of an event and might even yield information on terrorist attacks. The probability would be proportional to the price. Since people would be betting with cash, it was assumed that they would be more truthful.

The assumptions underlying FutureMAP were that human beings are rational economic players and that markets accurately predict the future. The model also assumed that information distribution processes are highly efficient, readily leveraged by players and that markets are free from manipulation.[35] All these assumptions may be questioned.

Moreover, unlike Presidential polls, which are scheduled to occur on a known date, the schedule for terror attacks is known only to the terrorists. Even if we assume that the target is known and that the terror event is certain to occur, the day would still be uncertain. The peak price would be no indication, since we would not know that it is the peak. Further, to assume that the information is so widespread that it has filtered into the market, is contrary to what we know of the way terrorists operate. If they allowed this to happen, they would be giving away information which could jeopardise their plans.

A more probable scenario would be one where terrorists pretend to be interested in a particular target. This would enable them to divert attention from the actual target and also enable them to manipulate the odds and the market. Research however indicates that attempts to skew the market only have a momentary impact.

The scheme could also be used by government to enable players to predict the death of enemy leaders like Saddam Husein. In such a case, the resemblance to Jim Bell's scheme would become very marked. In this case, players would attempt to bet on whether Saddam, Fidel Castro or Osama bin Laden would be alive on a certain date. In this case, the government's role would not be passive. It must be presumed that this would be linked to active attempts by intelligence agencies to hasten the demise of these individuals. The facts in this case would be known to the government and individuals would be betting on death dates. This would raise the same ethical arguments as Bell's scheme.

The exposure of Poindexter's scheme resulted in a huge outcry in Congress. The scheme was dropped like a hot potato, essentially on moral grounds.[36] However, some analysts feel that it could have been useful as a trend indicator and should have been continued, though perhaps not in the context of terrorism. In a study published by the AEI-Brookings Joint Center for Regulatory Studies, Professor Abramowicz concludes that information markets could help refine administrative agency predictions about government policy if the possibility of manipulation can be overcome. It, therefore, seems likely that FutureMAP may eventually resurface in an entirely different context as a policy analysis tool.

Conclusion

Jim Bell has suggested a scheme to punish corrupt officials which he calls DigitaLiberty. This presumes the existence of an organisation, which would allow those who correctly predict the death of such officials to be rewarded with untraceable cash, while keeping their identities secret. Discussion of his scheme and the eventual abolition of government, which he hopes it will bring about, require some rudimentary understanding of cryptography. Salient encryption systems have therefore been examined to understand better the issues at the heart of cryptology.

Bell's idea hinges on the use of PKC to preserve the anonymity of individuals who participate in the scheme. It also requires the availability of digital cash and digital pseudonyms on the lines suggested by David Chaum.

Asymmetric cipher systems together with the Internet form the cornerstone of Jim Bell's scheme of DigitaLiberty. It is truly revolutionary. It is a moot point whether it will be implemented. The dangers it poses to existing systems of command and control will probably ensure that it will never be. Bell argues that the system is not criminal. However, since implementation is likely to threaten elites, it seems very likely that laws will be updated to make such activity illegal.

The heavy dependence on advanced technology ensures that the system is not likely to be used in the developing world. While we cannot deny the devilish ingenuity of Bell's scheme, it seems most likely that it will merely be an interesting appendix in a book on the elimination of governments.

The Futures Market Applied to Prediction (FutureMAP) propounded by Admiral John Poindexter seems to have been inspired by Jim Bell's 'Assassination Politics'. The distinction is that it would be operated in the interest of national security. It would allow punters to bet on the occurrence of certain terrorist events like the likelihood of a terrorist attack, the assassination of a leader or the death of a wanted terrorist to obtain actionable intelligence on likely events.

Unlike Presidential elections, the time-table for terror events cannot be predicted. Terrorists are unlikely to be influenced by market decisions. That FutureMAP was under serious consideration only highlights the fact that no idea is too outrageous to be considered.

References/End Notes

1 "Amid Furor, Pentagon kills terrorism futures market" , 30 July, 2003, at http://www. cnn.com /2003/ALLPOLITICS/07/29/terror.market

2 Ibid.

3 Schlegel, Alex, "Jim Bell and Assassination Politics", at http://alex.creartivity.org/ articles/art-200109-assassination_politics.html updated July 30, 2003

4 Ibid.

5 Kahn, David, The Codebreakers: The Story of Secret Writing. 1966. Weidenfeld and Nicolson; London. p. xvi.

6 Ibid. pp. xiii-xv

7 Singh, Simon, The Code Book. 1999. Fourth Estate; London. p. 30

8 Kahn, David, no. 5, p. xiii.

9 Ibid., p. xv

10 Singh, Simon, no. 7, p. 31

11 Ibid.

12 Ibid., p. 17

13 Kahn, David, no. 5, p 84

14 Ibid., p. 46

15 Ibid., p. 49

16 Ibid., p. 51

17 Ibid., pp. 208-213

18 A working model of the Enigma is available at the site indicated below and will serve to give a good idea of how it functioned. See "Working Model of Enigma ciphering machine", Java Applet by Russell Schwager at http://www.ugrad.cs.jhu.edu/~russell/classes/enigma/enigma.html

19 Singh, Simon, no.7, p. 136

20 Ibid., p. 251

21 Ibid., pp. 264-265

22 Ibid., pp. 274-275

23 Ibid., p. 300

24 Chaum, David, Achieving Electronic Privacy. *Scientific American*. August 1992, pp. 96-101

25 Ibid., pp. 97-98

26 Ibid., pp. 98-99

27 McCullagh, Declan, "Crypto-Convict Won't Recant", April 14, 2000 at http://www.antioffline.com/apol.html

28 Bell, Jim, Assassination Politics", April 03, 1997 at http://jya.com/ap.htm.

29 Ibid.

30 Ibid.

31 Ibid.

32 "Amid Furor, Pentagon Kills Terrorism Futures Market", July 30, 2003 at http://www.cnn.com/2003/ALLPOLITICS/07/29/terror.market

33 "John M Poindexter" at http://www.warblogging.com/tia/poindexter.bio.html

34 Berg, Joyce, et al, "Results from a Dozen Years of Election Futures Markets Research", University of Iowa, November 2000, at http://www.biz.uiowa.edu/iem/archive/BFNR_2000.pdf

[35] Ritholtz, Barry L., “Terrorism Futures Market: Much Ado about the Wrong Thing”; The Big Picture: Macro Perspectives on the Capital markets, Economy Geopolitics, August 02, 2003 at http://bigpicture.typepad.com/comments/2003/08/terrorism_futur.html

[36] “Terrorism Futures Market Plan Cancelled”, Fox News Channel, July 29, 2003 at http://www.foxnews.com/story/0%2C2933%2C93190%2C00.html

Wg Cdr R. Sukumaran is a Research Fellow at IDSA. He is an Air Force fighter pilot and has operated on both *INS Vikrant* and *INS Viraat*. His research interests include military history, technology and the use of air power.

Errata: The name ‘Lt Cdr Frank Taylor of the Royal Navy’ on page 50 of the Jan-Mar 2004 issue of *Strategic Analysis* should read ‘Lt Cdr David R. Taylor of the Royal Navy’.
— *Editor*