At the threshold of the new world or How much do human thoughts cost?

For thousands of years our civilization has developed from a primitive society to capitalism and socialism, incidentally surviving the slave and the feudal formations.

The change of stages was accompanied by mass upheavals in societies, economy, politics, culture, religion and people's minds.

The evolution of the social system often caused degradation of culture and even the loss of accumulated knowledge.

Just remember the Middle Ages. The great poets and scholars of the Roman Empire were replaced by religious clerics; they imposed obscurantism and cruel Inquisition instead of culture and science. Even the living conditions indicated the signs of degradation: an ancient urban sanitation system was forgotten, and the Emperor Louis XIV, called “the Great”, had to use a chamber pot, when he lived in the Versailles Palace...

The consequences of scientific and technological progress also didn’t vanish without a trace. The first in the history of mankind Industrial Revolution resulted in peasant revolts and filled all Europe with blood.

The Second Industrial Revolution, which began in the XIX century, caused two world wars, repartition of the world, the creation of weapons of mass destruction, the emergence of the Internet and the new virtual reality.

At all historical stages the ruling elites have sought to impose a new order, manipulate people’s minds. They even tried to control their thoughts. Thus they could control a crowd during socio-political and economic transformations, making it obey like a slave. Maybe the civilization is on the brink of another social explosion and the third industrial revolution?

The emergence of the Internet and the progress of computer technologies changed our lives so much that it’s time to talk about global reassessment of traditional values of the civilization and the rise of the new order, based on the realities of the information world.

What is the difference between the new information reality, the largest part of the Mankind lives in, and the material world turning into a matter of the past?

As acknowledged by the inventors of the Internet Bob Kahn and Vint Cerf, they hadn’t considered the safety of their offspring, and therefore they admitted: “A new version of the Internet might be the best way to defend against cyber attack.” Let me remind you, that this technology doesn’t exist and is not expected in the next decade.

If we recall that the draft of the global information network was born in secret American research laboratories to communicate during a possible nuclear war, the sincerity of Vint Cerf and Bob Kahn, the "fathers of the Internet", is, of course, questionable. It is unlikely that they didn’t think about the safety of the top-secret military technology. Most probably, the "bugs" were deliberately created in the network to control users’ actions in future.

It justifies the fact that there hasn’t been any clear user identification ever since the establishment of the global network.

Such selflessness is still the major risk for the information world, because hackers and fraudsters can anonymously and thus unpunished gain access to any network and users’ resources.
Special backdoors for hackers in the Internet, absolute impossibility to provide the security of personal information and, most important, weak user identification – we do not understand where information comes from, where it goes, who uploaded it and who changed it - all these factors jeopardizes not only philosophical and moral but also economic foundations of the society. They encourage crime, suppression of freedoms and democracy.

It’s impossible to track information flow and understand when hackers have invaded the network without reliable identification and authentication. We are defenseless in the Internet. Being unidentified in the network attackers can compromise a person with impunity downloading any text in his computer or a mobile phone or sending an SMS message, an E-mail or a voice message.

Once in your device, a modern virus can send the hacked text to attackers. It’s even more dangerous that the virus can modify the stolen text, adding words necessary to compromise a person, and publish the text in the Internet, social networks, electronic media, thus prompting loud economic and political scandals.

For example, not long ago hackers recorded a conversation of the Turkish Prime Minister Recep Tayyip Erdogan with his son Bilal. Allegedly, they discussed the scheme of the construction of an oil pipeline from Iran. The injection of information could cause significant economic, political and financial losses throughout the whole region. But a special government commission examined the circumstances under which that compromising information appeared and defined that it was a fake.

Hackers’ opportunities to distort information are expanding. The detection of a spyware virus Regin confirms this fact. That computer worm remained invisible for a long time, hacking emails and intercepting phone conversations. It could make screen shots, store passwords and covertly send the stolen information to hackers via the Internet or mobile networks. Regin hides in computers better than other viruses.

Experts fear that this is one of the first swallows, and it will be even worse, because the existing anti-virus programs can’t often detect this type of attacks.

It’s impossible to defend oneself against Regin and similar viruses with standard methods, because anti-virus software is allocated in the computer software environment it is protecting. Thus affecting the computer software hackers neutralize the anti-virus installed in a computer.

Experts from Kaspersky Lab stated that over the past 12 months 52% of Russian companies have become victims of DDoS-attacks. 49% of DDoS-attacks last 6 - 24 hours, so companies are suffering losses worth at least $500 million. Analyzing the prospects for the world development against the background of these problems, we can see a real apocalyptic picture of the future... Nevertheless modern technologies are still based on the information platform that poses a risk to users.

Reliable cryptographic equipment should be used that cannot be decrypted even by the government. It’s the only way to ensure information security in the Internet. But there’s a paradox in this regard. Even in the most democratic countries this equipment is available only for those who are holding high public posts. Government officials use sufficiently strong cryptographic hardware to carry out their work, but at the same time they cannot defend their personal information. The reason is that, first of all, according to the laws they have themselves adopted they are not allowed to safeguard personal information from the government. Secondly, should have the same equipment be available for all members of their families.

George Washington, the first President of the United States, said with sarcasm half-jokingly: "The government is not reason, it is not eloquence, it is force; like fire, a troublesome servant and a fearful master. Never for a moment should it be left to irresponsible action.”

Just think it over: it is still relevant today. Many governments of the world, true "masters of terror", have tried to intimidate criminals and terrorists with their decisions in the field of information security, but they’ve intimidated only their employees.

Even high-ranking officials in the hierarchy of the leading countries, those who have extensive experience in the field of information security, are frightened. The sensational resignation of the CIA Director David Petraeus is an illustrative example. The fact that we had a mistress, a journalist Paula Broadwell, was discovered as a result of interception of their private E-mails.

The fear of applying strong cryptography to secure personal information completely compromised the reputation of the battle-field general, though he could easily ask his personal technical specialists to provide him with hardware encryption devices. But the general was afraid to use strong encryption for his personal correspondence so that no one could hack it. The danger of losing the highest public post and information leakage was less important for him, than the fear of using strong cryptography.
Even Recep Erdogan, the highest official in the country, the former Turkish Prime Minister and now the President of Turkey could not protect his private conversations!

Indeed, this is the information paradox of the contemporary masters of fear, the leaders of our civilization. They prefer leaving personal information of state and government officials open (even for hackers!) in order to control their subjects in future, but they don’t want to use strong encryption to protect it!

It is assumed that nowadays it’s impossible to manage civil servants without public control. But what about the other realities of the information world such as cyber terrorism and electronic espionage?

It is a known fact that not only public services, acting in accordance with their countries’ laws, but also criminals can control a person who has insecure private information in the Internet. The power and the efficiency of technical means criminals are armed with is strong as those used by state security agencies.

Can’t help but recall the phrase the great Russian poet Alexander Pushkin wrote two hundred years ago: "... The idea that someone overhears you and me infuriates me ... It’s very possible to live without political freedom; it’s impossible without family inviolability; penal servitude is not much better…”

It's amazing that the words of our outstanding philosopher are so important today. Our entire civilization can shatter against this cornerstone and fall into an abyss.

Here’s another amazing example. The US Central Intelligence Agency has recently decided to clean up their electronic archives. It’s interesting that all messages concerning low rank employees had to be destroyed in seven years, but information concerning 22 top officials had to be kept forever!

The question arises: who controls government officials, monitoring senior government officials’ information? Is collected information secure? Edward Snowden’s case shows that there are no clear answers to these questions even in a technologically advanced country like the United States.

What an amazing change the world has recently undergone! After all, not so long ago strong cryptography played a crucial role in the emergence of the greatest in the world democracy of the Western civilization.

Thomas Jefferson, an outstanding political leader and the author of the Declaration of Independence of the United States believed that the use of strong cryptography had helped to win the struggle for independence and establish an independent state. Not even the government (the British government, at that time) could decrypt it.

Why is modern democracy degrading instead of moving forward? Why is it turning to a different development path, which is either information communism, or information capitalism, or information slavery? And where will it take to in the nearest future?

The world we live in

People are faceless in the Internet today; but facelessness was also the characteristic feature of the society in the times of slavery. Slaves and peasant serfs had only by-names and nicknames. They had no right for authenticity and uprisings against slave-owners were the only way they could declare about themselves.

Most of the people in the information society haven’t advanced to the next step of social development, as, for example, after the collapse of the Roman Empire. But they have lost lots of scientific and technological achievements, degrading to the most primitive level - slavery (information slavery, of course).

Online hunting for users’ personal information is prospering in the Internet; unpunished hacking jeopardizes the existence of the cornerstone of the civilization - the concept of confidentiality of human thoughts. Secrecy of thoughts has always been considered to be inviolable not only from the point of view of democratic principles of individual freedom, but also from the theological point of view: only God had the right to read our minds.

However, modern science doesn’t stop the attempts to penetrate into the holy of holies of our mind and control this final frontier. It’s impossible to distinguish the consciousness of a living person from information in a robot’s electronic brain.
For example, a group of neurobiologists and neurophysiologists at the University of California developed an algorithm that could decode the inner voice of a man, that is, human thoughts. They managed to confirm the hypothesis that similar mechanisms are involved in speech and thoughts. A detailed report on the study was published in the

journal *Frontiers in Neuroengineering*.

The researchers admit that the developed algorithm is far from perfect. "We've got shocking results, but it is not enough so far to create a full-fledged device." However, it is a big step towards the development of a device that can "read" a person's thoughts.

Experiments with direct decryption of signals from the human brain continue, voice and text files, the derivatives of human thoughts, are already under the control of computer spyware, monitoring every word, every phrase in the Internet and telephone networks.

Computer spyware, tracking every word, every phrase in the Internet and telephone networks, has already gained control over voice and text files, the derivatives of human thoughts. Electronic chips, implanted in human bodies, will receive commands from our brain. They've already been designed and are now prepared for implementation.

But what guarantees, that along with the advance of scientific and technical progress these chips won't become mandatory and scientists will not teach them to receive and give away commands, changing our mind in the right direction?

What will happen, if cyber criminals use old flaws in the security systems of new chips? An ancient Chinese philosopher Confucius was right when he warned us fifteen hundred years ago: "People go to jail when words lose their meaning."

In fact, under the present-day laws, a person should be responsible for the information he is sending from a computer and mobile networks, if this information contains any threat for the community. Therefore, it's very dangerous that hackers can distort our personal information to such an extent that the state may consider it to be a threat to its security - and punish an innocent person.

Under existing laws a wrongdoers' victim can be imprisoned for many years if criminals substitute or distort original information. At the same time the punishment for the authors of dangerous viruses and hackers, using such software, may be far less strict.

With the emergence of the Internet private information, thoughts and everyday life of a person is reflected in social networks and forums. Private videos and photos, posted on various websites for free messaging and communication, are the basis of the information world and its main content.

There are no systems in the network that can evaluate personal information and the ways to secure it. It's one of the main contradictions of modern society and the source for the ongoing global information warfare and mass hacker attacks.

Will anyone make an effort to secure something, which is assumed to cost nothing?

The Bible clearly defines the value of our words: “In the beginning was the Word, and the Word was with God, and the Word was God. (Jn. 1.1).
Our mind has always been and continues to be an imperishable value and a unique feature of human beings. We use words and text to express our thoughts and feelings and to share information with the others. No one but God can know our thoughts. It's important in the information world that we can control our thoughts, when they are put into words and texts.

This postulate is particularly relevant in light of the experts' forecasts. They predict that 25 billion "smart" devices will appear in our lives in the coming years. They'll be interconnected in the global information network, linking the human brain with life support equipment, housekeeping, entertainment, work and medicine. This system will put a man on the machine level, and a machine will be put on the level of a human being.

IBM specialists tried to analyze what would happen with computers, smart phones and other gadgets in the next five years. Very soon computer equipment will be able to read the human mind. A forecast like this sounds really frightening. In five years it will be enough just to think about the subscriber to call him over a smartphone, instead of pressing a key or a touch screen to dial his number. Of course, new horizons will open for those who print a lot of texts manually. These technologies will help a machine to hear our thoughts at any point and they will start flowing into the Internet...

"Smart" devices equipped with artificial intelligence will also be able to think independently. Shall we manage to protect a person's individuality from robots' influence, if information networks are insecure and there are no laws that can guarantee privacy of personal information?

According to Symantec, hackers' annual profit has already reached $ 400 billion, exceeding illegal profits of drug traffickers and arms dealers. Why?

Sometimes cybercriminals' technological equipment is much more efficient than that of special services. Hackers can buy powerful graphic computers with processors, capable to decrypt tens of billions of passwords per second. Experts have estimated that in 2015, using these means of computation, criminals will hack almost all E-mail and social network passwords in the world. Just remember: some 2-3 years ago this equipment was available only to secret services working in the sphere if information security. Can you imagine the real force of hacker attacks if they unite in large groups operating all over the world?!

It's impossible to resist online attacks without strong cryptographic equipment, because it's the only reliable way to defend the information networks from any outside influence. Here's an example from my own experience. It has already become classical. It will help an uninitiated reader to understand that the statement above is not just a high-flown talk. The example below demonstrates that strong cryptography can disarm the smartest hackers and prevent the most extensive hacking attacks, involving information theft.

Everyone remembers the scandalous "Fake Letters of Advice". Criminals used them in the early 1990-s to steal several trillion rubles in cash from the Bank of Russia! That was the largest ever hacker attack on the banking and financial system of the entire country. If the way to stop the lawbreakers hadn't been found, Russia would have risked total financial collapse and a breakdown of the banking system.

Our super strong encryption device, designed according to the TEMPEST standard entirely on the domestic element base, made it possible to save the situation and stop the robbery of the Central Bank of Russia. The cryptographic system, created with its help, has been safeguarding information security of this major Russian bank for 23 years. The reliability and the extended working capacity of the cryptographic system have already proved that cryptographic equipment can effectively defend against hackers and forces they are backed by.

However, business owners and state structures neglect the use of cryptography, and the number of personal information thefts and hacker attacks on government and commercial institutions is growing at a great speed.

Experts on Information security state that 100 hacker attacks are conducted on average every second around the world. Every 4.5 seconds one of them causes substantial material damage to users. In a situation like this can users of electronic gadgets feel safe and be legally responsible for everything what is happening with their electronic data?

Remember a sensational example. A few years ago the government of Germany launched spyware into its citizens' computers, known as a "Bundespost Trojan". It was downloaded into a computer of an unknowing user and made it possible to do anything, for example, download new malware, steal passwords or make a photo of the computer owner with a built-in camera at the most inopportune moments.

The authorities had planned that the computer spy would detect terrorists' correspondence and report it to special services. It's interesting that a private company designed the virus upon the instructions of the government. Protests began and the project was closed only after people in Germany had learned about it.

This example demonstrates that public services often contract the development of information control and interception systems to private companies, and it's more difficult to control them. In a situation like such covert collection of personal information on citizens, organized by state organizations, doesn't defend them, but only exposes them to the danger of cyber terrorism.

If Internet and mobile network users are almost completely deprived of the rule of law and security, not only criminals, but also individuals striving for power may be tempted to use the forbidden fruits of technological progress.

Remember pre-war Germany. Hitler started the ascent to the top of power in 1928 with the help of interception of the political competitors of the future Fuhrer and the members of the German government, organized by Hermann Goering. He collected compromising material on the elite of the country employing German special service agents for that secret job. It helped Hitler to rein the most influential and wealthy people in the country, and Corporal Adolf Shikelbruger, an Austrian citizen, become a German Chancellor.

In 1933 Hermann Goering founded an Institute to control telephone and telegraph network and radio in Germany; that Institute received an official status. After Hitler had come to power that institute became a direct participant of all crimes of the fascist regime, including the organization of the Holocaust. During the war the Herrmann Goering Institute of interception was under the wing of the Ministry of Aviation and was called a Research Bureau (FA).

Unfortunately, the world has forgotten this fact, and even at the Nuremberg Trials the Goering interception Institute was not recognized to be a Nazi criminal organization. Was it a paradox? It wasn't in that case. Condemnation of the Nazi secret organization would have resulted in the investigation of its activities. Such turn of events was not profitable for the mighty of the world. The archives of the Goering Institute of interception contained the records of Stalin’s, Churchill’s and Roosevelt’s conversations. They were afraid that after the investigation the decrypted conversations could be published in open press, and no one wanted to advertise secret negotiations with the defeated tyrant.

At the same time Albert Speer, the Third Reich Minister for Armaments and Munitions, dared to declare about that danger. Speer was one of a few Nazis at the Nuremberg trials who admitted the criminal activity of the regime he’d served for. Besides during the war he was closely connected to a secret organization Ahnenerbe. Its Second Department was working intensely on changing human consciousness with the help of sound transmitted over radio and telephone.

After the armaments used by the infantry, the navy and air forces, the power over the human mind has actually become the fourth military power of Nazi Germany, which Hitler relied so much on in his struggle for world domination.

One of the methods, used by the "researchers" at the Second Ahnenerbe Bureau to establish control over the human mind, was erasing acquired memory and replacing it with memories appropriate for their leaders.

The Nazis used special code sounds for these purposes, disguised as different genres of music, especially military marches. How many people were involved in massive experiments on human consciousness in Nazi Germany? We can only guess today. But how can we explain why German citizens, intellectuals and workers among them, who’d supported communist and democratic ideas, were willing to accept Hitler’s nationalist idea «Drang nach Osten!» - a breakthrough to the East and the subjugation of peoples in Europe? It’s a telling fact indeed Unfortunately, judging by publications in press, similar experiments on human mind and thoughts control are still under way.

Several groups of neuroscientists from around the world have recently reported at the same time that they had developed a method to erase memories from human mind. Up till now in most of the countries experiments have been conducted only on animals. But, according to press reports, in 2007 American researchers at Emory University (Atlanta) started involving volunteers in the experiments, which were rather successful. Elizabeth Loftus, a professor of psychology at the University of California and the University of Washington, one of the leading experts on psychological mechanisms of the memory, said: "Psychologists have learnt a great deal about the nature of false memories. In the next 50 years scientists will learn how to create them artificially. But I am afraid that in 2084 a descendant of George Orwell will write a book about a totalitarian society where power controls memories. We must bear in mind that memory, like liberty is a fragile thing."

It’s interesting, that the researches on false memories made Elizabeth Loftus famous. During her experiments she demonstrated that it was possible to make a person "remember" what he’d never experienced in his life. The participants found stories in their memories of getting lost in a supermarket when they were children or cutting a hand deep with a glass, though it had never happened to them.

False information and disinformation of any kind can damage our real memory; it may happen when we are talking to someone or, for example, reading newspaper articles on the events that we have witnessed.

The researches of contemporary tamers of human consciousness are not yet widespread, and formally pursue purely medical purposes. In particular, they are trying to find a way to relieve mental disorders associated with tragic events in a person’s life. But where is the guarantee that the established mechanism of changing consciousness won’t be used on a massive scale for entirely different purposes, which are far from medical purposes, as the researchers tried to do in Nazi Germany?

For example, what’s the cost of the apologies made by the management of a social network Facebook? They officially admitted that they had conducted a secret psychological experiment on their users to adjust their mood. What was the essence of the experiment?

According to the press, the experiments took place over the course of one week in January 2012. There were 689 000 participants who received posts, and two groups of users were analyzed. One of them received posts containing only negative posts and the other received only positive posts.

According to the authors of the research, initiated by Facebook, users’ mood changed depending on the news: those who’d received a negative post, wrote rather negative comments; and those who’d read positive news, shared their wonderful mood.
A newspaper *Mercury News* quoted the researchers: "The result showed that the emotions of other people have a significant impact on other users". It was also observed that the emotions received from the pages of the network could influence a person and people around him even after access to the profile was disabled.

But worst of all, hundreds of thousands of people around the world were involved in the experiment without notice and consent...

Speer admitted in his final statement to the Nuremberg Tribunal:
"Hitler’s dictatorship differed in one fundamental point from all its predecessors in history. His was the first dictatorship in the present period of modern technical development, a dictatorship which made a complete use of all technical means in a perfect manner for the domination of its own country.

Through technical devices like the radio and the loudspeaker, eighty million people were deprived of independent thought.”

Note that Speer called Hitler’s dictatorship not the last but the first dictatorship in the world that used the potential of scientific and technological progress not for the benefit, but for the destruction of the foundations of human consciousness.

Unfortunately, at the end of the bloodiest war in the history of its existence our civilization hasn’t learned any lessons from the events prior to Hitler's assent to power, and Speer’s declaration was not taken into consideration.

That’s why we can’t be sure that tomorrow another dictator won’t use interception and compromising material to pave his way to power.

Besides, the concentration of information has increased a million times, and now it’s easier to gain incriminating evidence.

Ongoing information wars and total wiretapping worldwide continue their disastrous march, and no one in the world today can guarantee that new "Hitler" led by hackers’ dictatorship wouldn’t appear on this path.

Crime without punishment

Is it possible to punish hackers for our stolen or destroyed intellectual property and receive financial compensation?

We’ve already seen that when a text is created in a computer, a user is fully responsible for its content. It doesn’t matter that it’s not signed by the computer owner. The electronic tags of the "instrument of production» - an ID processor installed on a PC, a device serial number, etc. – indicate the author. But who is responsible for information and its security while it is transmitted over information networks? After all, we’ll not receive compensation for any hacking attempt if our texts are intercepted, stolen or distorted, but we’ll bear responsibility for the content someone has distorted!
Sending information from his PC to another PC a person is considered to be the author of the information. He is responsible for the content. At the same time he is not considered to be the owner of personal information, that is, of his own thoughts! It doesn’t matter in this case, that we pay a provider for his services. He never takes the responsibility for the safety of the transmitted content.

This casuistry causes another huge problem of the modern society - the low level of information security.

Indeed, why should providers or manufacturers of information technology equipment spend money to defend personal information if it doesn’t cost anithing?
Strange as it may seem, people accept it. They’ve been taught that, allegedly, no one needs their personal information and it isn’t worth a penny. But note: Internet giants massively collect metadata about individual users and use them to increase the efficiency of advertising sales. It’s another example, demonstrating that our personal information has its own price, and its value is high.

But, bearing in mind the anonymity of the global network and the imperfection of modern laws, it’s almost impossible for ordinary citizens, hackers’ victims, to restore their reputation. When we register in any online service, we automatically sign an agreement. It is legally specified there that the owners of these services refuse responsibility and possible users’ claims. That is, we haven’t yet begun to use electronic services, but we’ve already given the indulgence to our potential plunderers.

Lack of legislation and upside down psychology

Most recently I’ve led the delegation of my company at one of the largest exhibitions in the field of software and computer equipment. We demonstrated an encryption device designed by our company which had no analogues in the world. Many people - government representatives from various countries were the most frequent visitors to our exhibit booth – came up and asked, whether the specialists who had designed that unique encryption device, could also consider decryption issues.

You should have seen the reaction of people when they heard in reply that information security and data mining are incompatible neither morally nor legally, when it comes to commercial organizations! They’d better apply to the appropriate state services in their countries about it...

Today hacking psychology prevails in the world over the traditional democratic values with their roots in the Bible. People are rarely embarrassed to hunt for someone else's information. Not only observations at the international exhibition, but also dry Internet statistics confirm these facts.

Alongside with the description of the functions of our encryption device on our website we've published information, characteristics and features, on various types of spy equipment designed for mobile phone interception. Manufacturers of this equipment publish this information in the Internet and it's available for public. Naturally, we haven't specified their addresses and the trade names of the models. We only wanted to show people that there were lots of possibilities in the world to wiretap mobile phones and it could be done easily.

Frankly speaking, the readers' reaction surprised me so much. The detailed analysis of numerous requests from our website - their number has exceeded ninety thousand – showed that three quarters of these responses contained a request to purchase an interception system. Only one quarter of the readers were interested in our encryptor as a device, that could defend personal and corporate information.

Imagine, one quarter of the readers wants to defend their privacy, and three quarters want to wiretap their fellow men!

It's not just the change of mentality in a small group of people. Referring to the wide-scale statistics and its geography, one should consider the changing moral attitudes of the society as a whole.

Scientific and technological progress opened a Pandora's Box: any electronic technology is available everywhere now, but ordinary people are mainly deprived of essential tools to prevent hacking and cyber-terrorists' threats.

Users are insecure in the Internet, that's why it turned into real Klondike for hackers, who can make illegal money there.

During the Gold Rush many people came to Alaska from all parts of the world to get rich quickly. They didn't have good education or profession. They can be compared to hackers: they also use computers and the Internet to pick our electronic wallets and dig out compromising information by the order of criminal clans.

Legends about fabulous profits in this pirate business attract more and more young inexperienced people. Hacking large public and commercial networks, as well as computers of famous people, they feel imaginary greatness, creating an imaginary aura of significance around them; and alter egos of the so-called "hacking fraternity" support them in every possible way.

Almost total impunity of Internet pirates makes such activities very attractive for young people.

The problem of detection and punishment of hackers, who attack electronic resources of VIP-persons or large organizations, is resolved a bit easier. Against the background of great scandals in the media, flaring up after every hacker attack, criminals are captured as a rule. But it's an exception rather than a rule. Stolen or false information on prominent persons, published in the public domain of the Internet, can cause not only extensive press coverage, but also negative financial consequences for the market as a whole.

Here is an example. Twitter was hacked and a bogus report was published in of one of the information agencies that Barack Obama had been wounded. As a result there was a sharp fall in the American stock market.

Cybercriminals, hunting for computer data, know this is a profitable business, so they’ve expanded the scope of their activities and intensified hacking social network accounts of well-known users. The cost of this account, in the case it’s resold, may immediately reach tens of thousands of dollars.

The expansion of criminals’ interests in the Internet has become a kind of a trend. If you remember, a new Regin virus is also omnivorous and universal. It collects information on all subjects on a massive scale: finance, technology, economics and personal accounts in social networks not only of government officials, but even of businessmen and heads of industrial enterprises. Note: hackers are now interested in industry as well! Their priorities have changed. They discover more and more profitable niches in social networks and personal accounts of citizens. It proves once again that modern copyright laws in the Internet don’t defend ordinary users.

However, the owners of Internet services and equipment manufacturers, who don’t provide security for the users of their paid services, along with the criminals, who’ve hacked them, should bear financial responsibility for our compromised accounts. Instead of investing in information security and ensuring the safe use of new technologies, the “guardians" of our information officially warn us that there are no guarantees in this situation. We are embarking at our own risk on a dangerous path, leading the humanity into the wild information jungle...

Contemporary methods of total control over citizens, which are used, , for "crime prevention”, as security services claim, remind of a story "Fahrenheit 451", written by the great American science fiction writer Ray Bradbury. He describes future America - a totalitarian society where literature with clever ideas is forbidden and firemen burn all prohibited books and spy on the owners of "suspicious" texts, instead of fighting fires...

The author portrays people who’ve lost contact with each other, nature and the intellectual heritage of mankind. They hurry to work or back home; they don’t speak about their thoughts and feelings and discuss only nonsense and admire only material values.

They have interactive TV at home, a kind of the modern Internet, and spend their free time watching endless and useless series on TV. However, the state which seems to be "trouble-free", at first glance, is on the verge of a disastrous war, destined to start at the end of the story...

It was written back in 1953 but, unfortunately, the situation described has almost become a reality.

Here’s an example - a recent speech by the FBI Director James Comey to the representatives of big business. What did that distinguished American citizen say?

It turns out that the head of a state organization which should provide the security of taxpayers at their own expense, called on the companies, manufacturing gadgets, to abandon encryption of users' personal data, so that the FBI could have unlimited access to all private information.

Justifying the FBI request, the Director of the secret service called on the manufacturers of electronic gadgets and software to help the FBI in its investigation.

However, Microsoft, Google and other major phone and software manufacturers didn’t support Mr. Comey. They realized that as a result they could quickly lose their customers.

James Comey also complained that after Snowden’s revelations Americans used antispyware technology more actively, trying to secure their personal information. Mass media cited Comey, saying that if that trend continued, the FBI simply wouldn’t be able do their job.

The world learned from Snowden’s revelations what kind of job it was: technology companies collaborated with secret services to collect (i.e. steal) users' personal data in the Internet.

According to *The Intercept* online edition, Snowden’s documents show that the Aurora Gold program helps the NSA to gain access to each mobile operator in the world. Using this program US intelligence agencies control the methods used by cellular companies to secure their customers’ private data, and the possibilities to bypass security systems.

According to one of Snowden’s documents, by May 2012 the US intelligence received technical information on 701 out of 985 mobile networks in the world (i.e. 70%!). The NSA also spied on an influential British organization GSM Association, an association of mobile operators. Russian operators, MTS, "Megafon" and "Beeline”, are also the members of this organization. The NSA actively monitored the content of E-mail messages, sent over the mobile networks, and the accounts of 1200 managers of these networks.

Snowden’s documents show that breaking security systems for its special agents the NSA opens the doors for hackers and gives them access to systems, which store and transfer users’ private information. What is really important for intelligence services? Of course, they want to know the real situation, enter criminal structures, reveal their secret information and deprive them of financial sources.

The FBI Director’ suggestion to spy on criminals on the Internet is just contrary to such working methods, which lead them into virtual reality. Let the respected law enforcement organization wedge in criminal networks, capture encryption keys used by terrorists and get information, rather than report the number of wiretaps.

Intelligence work is, probably, the most effective way to fight crime and terrorism. At least intelligence services will be able to get information from the real sources on the customers of crimes, and, most importantly, on those who finance them. It’s unlikely that after public statements, made by special services representatives, terrorists will continue using sophisticated electronic devices to communicate over the Internet or store secret information there. An amazing detail was found out after terrorist №1, Bin Laden, had been captured: he didn’t use any encryption at all...

Who is responsible for the staggering growth of hackers’ incomes?

According to the information announced at a special meeting of the British Parliament, hackers' incomes have already exceeded 400 billion dollars a year! What helps criminals to earn huge amounts of money?

The first thing that comes to mind is our helplessness, both legal and technical. There are no laws that guarantee the security of private information, and self-security which may be provided by strong encryption is limited. Doesn't it confirm Ray Bradbury's gloomy predictions?

There's another significant issue increasing the level of criminal danger in the information world. Do you know what experts, those who've spent a lifetime mining data, do after the retirement from state service? Where do they go? It won't be a big surprise if it turns out that they are immediately noticed by criminals. Their profits are huge, so they can pay these experts much more than they earned at state organizations.

Permanent inflow of highly skilled professionals into international criminal hacker clans is one of the most important reasons for the surge of electronic crime, posing a threat to democratic rights, freedoms and the material well-being of Internet users.

Active dissemination of spyware all over the world, instead of programs providing data privacy, shows that, unfortunately the world leaders don't realize the terrible danger looming over our civilization. Criminals don't even need to be present at the scene of the planned crime. Everything is done remotely, thousands of miles away from the target, using just a keyboard of a computer connected to the Internet.

For example, the Baku - Tbilisi - Ceyhan oil pipeline is built according to the highest standards. It's equipped with sensors and cameras, monitoring virtually every meter of the pipe - from the Caspian Sea to the Mediterranean region. The explosion in 2008, just a few days before the war with Russia, disabled it for a long time, but not a single sensor fixed it.

Western intelligence services, which investigated the incident, came to the conclusion that not Russian fighter jets but hackers were to blame for the explosion. They turned off all the sensors and it caused overpressure in the pipes and then the explosion.

There was no need for the criminals to hack the central computer: they penetrated into several computers located at the auxiliary pipeline control stations. Their goal was to receive access to the management of the pipes and increase pressure in them.

The incident with the oil pipeline is only one example, which demonstrates that without adequate encryption the Internet networks and modern communication technologies are posed to danger.

Bloomberg's Jordan Roberston and Michael Riley reported that information security experts had prevented a cyber operation, targeted at the commercial airlines of one of the countries.

It is no secret that hackers can carry out cyber attacks on airliners and flight control systems, change aircraft routes, make two airplanes dash or hit objects on the ground. Reports on such successful attempts haven't yet appeared in press, but still it isn't clear, who guided the planes, high jacked by terrorists, to the Twin Towers in New York on September 11, 2001, and why the Malaysian airlines Boeing vanished from the flight path. Cyber terrorists can dismantle life support medical electric equipment and even deorbit satellites... But it’s only the beginning.

Clans of thousands hackers can unite in an instant and take over the actual control over the entire life support system all over the world. There’ll be no one to blame for it. For the sake of someone's political and economic interests Western democracies have created a situation when equipment is made use of, which doesn’t provide strong encryption.

In the mid 1980-s, having realized the threat of nuclear weapons proliferation, hanging over the planet, the leading countries adopted a consolidated decision to control the design and experts working in the spheres related to the development of nuclear weapons. Today all the ways are open for information weapons specialists when they quit state service. There are no restrictions for them.

The same is true for the proliferation of spy equipment. The most advanced electronic spy equipment is shipped for a long time to many African or Latin American countries with unstable political regimes. There’ve been no problems yet. But what happens to this equipment? As a rule the latest technologies disappear in a "black hole” after a coup or revolution. They flow away to criminal organizations or terrorists, to be more exact. We’ve seen a similar situation in Libya, Iraq and other countries. In this regard the international community has, of course, to revise the existing international laws and restrictions.

Can hacking defeat evil?

Who will stop the hackers’ empire and how is it possible to do it, if there hasn’t been a legal and economic base necessary to combat them for a long time?

If criminal organizations have state of the art equipment and professionals who perfectly know of all secrets of the security services, there’s no use fighting them with the same weapons, monitoring and stealing information. Hackers are well trained in a job like this and can easily bypass the traps set for them.

While intelligence agencies wiretap the whole world hoping to detect terrorists, the latter are silently wiretapping special services using the most advanced equipment and gather any kind of information they are interested in. No one can stop hacking outrage in the Internet as long as we witness the surge of spy technology and almost complete lack of cryptographic protection. We can only state that the development of information technologies that used to be the engine of the civilization, have suddenly become a powerful weapon, posing a threat to the civilization.

By the way, history has already given a negative answer to the question whether it’s possible to defeat online pirates with their own methods. Let’s remember that in the XV - XVII centuries England hired pirates to defeat the strong Spanish fleet. That tactic caused losses to the Spanish explorers and incredibly enriched corsairs, who became much stronger than the naval forces of the British Empire.

If the processes in today’s global information space continue developing at the same pace, if the hackers’ profits increase, all governments may face enormous political, economic, legal and, even more, moral and ethical problems in the near future. We are standing on the threshold of a global information war, equivalent to a nuclear war by its might. Electronic information is anywhere. Using a computer and Internet access it’s possible to disable a nuclear power or a chemical plant, hijack a plane. Everything is controlled by computers now.

In fact, the situation around the world shows a new form of society - the dictatorship of information. And if the prevailing world order is not re-thought, the lack of laws and technologies, which ensure users' security, may lead the world to the dictatorship of hackers and those who are behind them. Then anyone - a religious fanatic or a fascist - can become a new ruler on the Earth.

The world has to make a new choice today. Let's decide what's more important for us - freedom of information, based on the recognition of the value of private information, or the dictatorship of information, stimulating a ban on information security? I choose freedom!