The New Economy
Some New Threats to Security

Valeriu Tudor

Introduction

One can consider that the New Economy or Knowledge Economy or e-Economy, based on the Information Technology and Communications (ITC), may be defined as one that operates under different economic rules. In reality, such a New Economy does not exist. All new companies follow the same basic rule that share prices must reflect profitability. Like old successful companies, the new ones in the internet, media or biotechnology sectors can succeed only if they benefit from superior entrepreneurship. In fact, the really new successful companies in the Information Technology (IT) are no different economically from equally successful old economy companies.[1]

Mobile communication and the internet have undoubtedly had a tremendous impact on productivity and mobility for Western and some other economies as a whole. Their arrival has been an event of significant macroeconomic importance, though not comparable to technological breakthroughs such as electrification, the expansion of the railway or mass production all over the world.

As it is underlined in the Okinawa Charter on Global Information, IT is becoming one of the most potent forces in shaping this new century. As a vital engine of growth for the world economy, IT can serve the mutually supportive goals of creative sustainable economic growth, enhancing the public welfare, and fostering social cohesion, and work to fully realize its potential to strengthen democracy, increase transparency and accountability in governance, promote human rights, enhance cultural diversity, and to strengthen international peace and stability.[2]

The Information Technology proves to be a real high vector of globalization, with all advantages and disadvantages for all the countries of the world, since the international relations, including economy and trade, are still far from being based on principles and norms generally accepted.

The paradigm of the new economy is already challenged

There are views that rather than talk about the "knowledge economy" or the "new economy" it is more accurate to describe a "network economy" driven by ITC. According to these views, if the XIXth century was the era of the factory, the XXth was dominated by the office; the new century has a new driver of economic and social organization: it is called the network. This has given birth to a new phenomenon, the free worker, who is overturning conventional notions of the employer/employee power relationship and radicalizing the way workers are recruited, paid and kept happy as much as possible. The power of networks, the personalization of contracts, employee mobility and value of knowledge are already observable. The free workers are the fragments of the future here in the present.[3]

New human resource management

The e-economy has prompted employers to disperse with tradition and adopt a more people-based style of management. The arrival of the new economy based on e-commerce and information technology has made the traditional forms of work organization look even more obsolete to an educated and skilled labor force. As a consequence, a growing number of companies in the US, the UK and other countries of Western Europe have introduced new human resource management techniques underpinned by less hierarchical structures of decision-making emphasizing, team approach, job rotation, performance related pay, devolution of decision-making and employee financial participation. This experience suggests a new possible synthesis between business efficiency and social justice in the modern new economy enterprise. Such a growing evidence also suggests improvements in productivity, profitability and, above all, stock market valuation depend to a greater extend than in the past on how their own employees facing new Information Technology and e-commerce.[4]

Many of the ambitious young people who sought instant wealth by joining dotcom start-ups in the US are having a rude awakening. There are clear signs of a rise in the rate of their defection over the past months to more traditional brick-and-mortar companies. It does not mean the dotcom aspirants hanker for return to the "old" economy. They still want information technology jobs, but would prefer them to last longer. In other words, they want to have their share and benefit plenty from it.

What is becoming clear painfully is that there are simply not enough knowledge workers in the world to meet business demand. The shortage of available workers is already provoking an explosion in recruitment in e-commerce, with many employers anxious to rise pay levels well above current inflation rate to attract staff. But attempts to encourage the internationalization are not confined to senior management and information technology talent. It seems that in the UK a strong case for relaxing immigration rules can even be made on culinary grounds, because there is a shortage of Indian chefs. The benefits of the drain brain from other countries is a flourishing phenomenon with those who made early option for the new economy and internet companies.

The need to bridge the widening education gap between the information "have" and "have note" is one motivating factor for educators fighting the digital divide. Technology has the potential to bring valuable educational tools and resources to developing countries and inner cities, but building personnel can be costly.

The digital divide is much more than building the basic physical infrastructure needed to go online; financial access to the internet is just as important. The access to information is sometimes barred for some people by the excessive westernizing of the content on-line or by the use of the English language.[6]

The knowledge economy

As one of the main streams of the new economy is the knowledge economy, the developing countries are increasingly left behind as developed countries focus on high-tech products and services. The knowledge economy offers exponential returns on investment in education and will thus widen the gap between rich and poor nations. The latter, still struggling to promote literacy, are unable to invest also in higher, technology-oriented education programs. They are far from gaining a foothold in the knowledge economy. Nevertheless, they should not forget that no country can afford to refrain from technology-oriented educational investment, however urgent its basic educational needs. One example is the remarkable boom in India's software industry, with its highly trained computer specialists. This kind of education success story, like in South Korea and some other developing countries or countries with the economy in

transition, lies in their ability to make hard choices in allocating limited resources to different parts of education sector.

Targeted investment in high-tech fields and specialized institutions of learning must be balanced with investment in basic education for all. Many countries cannot hope to do everything at once, but they must be helped to put in place all the essential steps between basic and higher education, between literacy and high-tech research. If the connecting links between basic education for all and the high-powered knowledge economy is lost, there is a big risk of opening chasm between poor and rich countries. According to Kochiro Matsuura, "this is a lesson that no country can afford to ignore".[7] Above all, one has to understand that it would be to no one's advantage to allow the knowledge economy to break the world up into small islands of wealth surrounded by a sea of want. This cannot but be another factor of security or ... insecurity in a world of renewed challenges.

The New Economy versus the old one

In terms of efficiency, nothing is final. Indeed, when it comes to online commerce, the symbiosis between the new economy and the old one has deepened noticeably since the last two-four years. In fact, a spate of alliances and joint ventures between established manufacturers and companies specializing in electronic commerce has blurred the line between the two. As a result, traditional companies in a range of industries now look much better prepared for the promised business-to-business e-commerce revolution. Internet companies that have sprung to prominence on the promise of business-to-business innovations are starting to value their own relationships in the old economy far more highly.[8] Despite this, and even after recent gyrations in the stock market, investors still seem prefer new economy companies to more traditional ones. On their own, however, some prominent cases may not be enough to convince the stock market that the true heirs of the business-to-business revolution will be traditional manufacturers.

The corporate restructuring, repositioning and reorganization underway are reshaping the computing, communications and context landscape, being likely to emerge a new class of global heavyweights which will create, manage, control and distribute digital content in the internet era.

The internet and the mobile telecommunications

In this internet age, where speed is everything, many of the old economy rules seem to no longer play. Where time-to-markets becomes crucial, or human resources are in short supply, many companies are attempting to jump-start product development programs, plug product portfolio gaps or leapfrog competition by acquiring technology.

Another obvious factor reshaping the computer and telecoms industries is the dramatic growth of the internet since the mid 1990s. Now, the internet connects about 200 million people. This figure is expected to grow to 1 billion in a few years.[9]

The world is stepping in an age where a click of the mouse will seek out the cheapest product that suits the consumer's needs, all goods will become commodities and many familiar brand names will become meaningless.

The world population is about 6 billion people. They own an estimated 350 million computers, 450 million mobiles phones, 600 million cars and as many as 1 billion television sets. Sooner or later, all these devices and more will want to be on the internet.

The problem is there is no room, because the web is running out of addresses; all possible permutations of numbers will be soon exhausted. Internet protocol version 6 (IPv6), the upgrade to the present version 4, would allow for theoretically almost infinite number of addresses. Yet it has not been adopted.

As American companies were first to realize the commercial value of the internet, they were allocated a disproportionate numbers of addresses. The companies of other countries have fewer and they will require more. By 2003, the 600 million users on the internet will mean to go to IPv6. By 2005, probably, IPv6 will take over from IPv4 as the dominant protocol.[10]

The ability to offer speech as well as text and graphics on a web page is at the core of the emerging mobile e-commerce (m-commerce) and voice enabled e-commerce (v-commerce) markets. Instead of accessing the internet via a PC or interactive television, m-commerce uses mobile phones, palm computers, personal digital assistants and other portable devices. A prototype mobile device designed for m-commerce has been developed. The Nak (abbreviation of Nakulu, the Hawaiian word for *echo*) uses speech technology for sending and receiving e-mails, which are read by the user, making simple inquires thus be used by many people. So internet access through smaller devices will allow the voice to replace the keyboard.[11]

The astonishing growth of mobile telecommunications has helped create another tier of phone companies. According to some estimates, the number of people accessing the internet with mobile smart-phones and other handled devices will exceed those accessing the net using PCs within a few years.

Meanwhile, new technologies will enable much richer services, including video, to be delivered via wireless communications.

Whereas internet streamed media started on personal computers, it is already available through different devices, for instance the portable music players, then downloading direct to a mobile telephone. Third generation mobile telephone networks will provide enough bandwidth for audio and video streaming.[12]

The internet has turned out to be one of the most powerful forces shaping business for decades. But it also proved to be a fertile ground for speculation. Entirely new markets have been promised, with completely new ways of doing business and new ways of doing money.

Many new companies on the New Market of the ITC already face serious cash-flow problems at a time when their share prices are falling and their access to fresh capital is therefore restricted. The difficulties of that kind of companies remind "the idea of a structural break from the past is a lie, a marketing concept". That is why the amount of ambition of today's generation of managers cannot enable them to escape the rule that "when companies do not love enough money, they go bust".[13]

The ITC in the United States and the European Union

In the US, the ITC sectors, the core of the new economy, account for above 7 percent of the Gross Domestic Product. In the European Union, they make up only 4 percent of GDP, though this proportion is expected to approach US levels in the next four-five years. Investment in ITC is a little higher, at 7 percent of GDP, compared with 8 per cent in the US.

In the second half of the 1990s, the US ITC accounts for approximately three quarters of 1 percentage point increase in annual productivity growth. But in the European Union productivity growth has been lower, and the jury is still out on whether the continent can emulate US performance over the next few years.[14]

European Union leaders agreed, in March 2000, at the Lisbon Summit, a sweeping agenda of economic and social reforms. A major target was the creation of a vibrant European internet economy, closing the gap with the US in terms of employment and competitiveness. In their Lisbon declaration, they said the EU should "become the most competitive and dynamic knowledge-based economy in the world capable of sustainable economic growth with more and better jobs and greater social cohesion".[15]

To back up this "new strategy goal", European Union leaders made two dozen commitments to adapt their economies to the internet age, which include a legal

framework for e-commerce in 2000, full liberalization of telecoms by 2002, internet access for all schools by 2001, and W1 e-Europe Action Plan specifying targets for interconnected low-cost, high-speed internet and telecommunication networks in all EU countries.

The Nice Summit adopted new measures aimed at the implementation of these commitments. For achieving them, probably Europe should abandon its "fortress" mentality and follow America's lead in encouraging more inflows of labor, which, on their turn, are stimulating the brain drain from other countries, namely the developing ones and those with economies in transition.

Security issues in the cyberspace

In the G8 Communiqué Okinawa 2000 (Okinawa, 23 July 2000), there is a special reference to the theme: "We must take a concerted approach to high-tech crime, such as cyber-crime, which could seriously threaten security and confidence in the global information society. Our approach is set out in the Okinawa Charter on Global Information Society".

Indeed, the Okinawa Charter on Global Information Society underlines, *inter alia*, that international efforts to develop a global information society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. We must ensure that effective measures, as set out in the OECD Guidelines for Security of Information Systems, are put in place to fight cyber-crime. G8 co-operation within the framework of the Lyon Group on Transnational Organized Crime will be enhanced. We will further promote dialogue with industry, building on the success of the recent G8 Paris Conference "A Government/ Industry Dialogue on Safety and Confidence in Cyberspace". Urgent security issues such as hacking and viruses also require effective policy responses. We will continue to engage industry and other stakeholders to protect critical information infrastructures".[16]

This was a renewed warning, because the competent authorities in many countries have tried even before to counter increasingly sophisticated offenders in cyberspace. In the US case, according to Louis Freeh, director of the Federal Bureau of Investigation, the laws were not keeping up with the growing pace and sophistication of cyber-crime. Nonetheless, just as computer crime has evolved and mutated over the years, so too must our laws and procedures evolve to meet the changing nature of these crimes", he said at a Senate Committee in March 2000. In his view, "in the cyber equivalent of an arms race, exploits evolve as hackers design variations to evade or overcome detection software and filters".[17] And that was quite long before September 11, 2001 terrorist attacks in New York and Washington ...

Mr. Louis Freeh urged the Congress to support legislation known as The Cyberspace Electronic Security Act, proposed some months before by Justice Department to strengthen investigative techniques available to law enforcers and increase resources for cyber investigation. At the same time, he urged a review of current sentencing provisions for computing crime.

This hearing followed a global reaction against fraudulent internet schemes coordinated by the US Federal Trade Commission, and publication of a Computer Security Institute report showing the dramatic increase in the cost of computer crime in the US.

There was not a coincidence that before the hearing cyber-attacks were recorded on large sites, including Yahoo!, eBay and CNN, as a confirmation of increasing in frequency and sophistication of this kind of attacks.

Now, the information made available on the internet has become more than a concern because of privacy. Two or three years ago, companies weren't paying too much attention to this issue. Last years, the spread of "cyber-leaks" has emerged as one of the most serious new threats to corporate privacy, and a unique way for outsiders and insiders to break down the walls of corporate secrecy.

In 2000, some large mergers or merger discussions were leaked on internet messages boards run by Yahoo!, the internet company. In each case, the chater turned out to be true.

Once investors can buy and sell shares on weekends, when most cyber-leaks occur, stock volatility may rise even more than it has now, sparked by true, but more often false, speculation.

That is why many technology groups are developing software and cyber-sleuthing techniques aimed at tracking down messages, sometimes within seconds of aposting, and developing strategies for their corporate clients.[18]

Any concept of security in the information age should define the infrastructures which are so vital that their incapacity or destruction would have a profound negative impact on the defense and economic security. Among these vital infrastructures there are transportation, oil and gas production and storage, water supply, emergency services, government services, banking and finance, electrical power and telecommunications, food reserves, military objective and many other things.

The US history of the recent years provides a number of events that have served to heighten fear of exposure be they satellite failure which, for instance, caused half of the United States to lose its beeper service and halted companies ability to process credit card purchases, or a power outage in San Francisco, California, which left the city of San Francisco without primary power for six hours.[19]

Some risks and actions of terrorism in cyberspace

But in a digital world there are the risks and actions of the cyber-terrorism, which can be more dangerous than every missile, even a ballistic one. In fact the networks do permit launching terrorist attacks from any point on the globe, which can be directed towards any objective depending or being coordinated by the information influx.

The new forms of terrorism may also put in danger human lives, but in a more silent manner, acting as arms of mass disturbance, not of mass destruction. Nevertheless, without pulverizing the concrete structures or providing blood rivers, they can provoke serious disturbances and losses of every kind, both human and material.

In the case of the US, considered as a "system of systems", the networks were, at least some years ago, very vulnerable for terrorists good users of computers. They can disturb the communications and information systems and further financial and banking systems, energy systems and many other systems, including those of State Administration and National and Security systems.

It is already known that some terrorist groups and members of organized crime are using soft to codify their messages and so they cannot be easy supervised. According to William Crowell, former director of National Security Agency. If all the PCs in the world were used to decode one single message, it would be necessary a duration of 12 millions times more than the age of the universe.[20]

Not long ago, the press network on-line ABCNEWS disclosed that many informations concerning the locations. Plans and facilities at the disposal of presidential and military commander centers – real sensitive points of the American defense – were accessible to any internet user all over the world. It makes very easy to plan a terrorist attack against the U.S. These sites were, at least before 11 September 2001, very numerous, being built up and published on web by NGOs, experts and even the US Government.[21]

The terrorist attacks in the US put in a new light the vulnerabilities of the whole system based on IT. The globalization of the communications had a huge contribution to increasing the risks and vulnerabilities of the networks, and more precisely of the internet and computers. In fact, the virtual space is now becoming a battlefield, which can be easily used by hackers and most probable by terrorists. Among most possible use of

computers by virtual and real terrorists and other unfriendly users of IT, one can quote:

- Diffusion of hate messages.
- Yielding (gathering) information concerning a nuclear bomb building up or other data that can be used against the Governments.
- Access to research results in biotechnology, medicine and chemistry, seeking biological, chemical and nuclear weapons.
- Spreading of viruses meant to destabilize the Governments and private networks.
- Access to national military and security classified information.
- False alarm launching.
- Danger of breaking down the electricity and water supply.
- Spreading of false rumors and news able to deregulate the Administration, the Police, the Health Services, the Stock Exchanges and the Media.
- Diffusion of news and false rumors, that can provoke fear, insecurity and so on.

In the US, FBI in close co-operation with industry, namely System Administration, Networking and Security (SANS) Institute, proposed a list of some 20 most dangerous security breakthroughs in the internet. Now, FBI and SANS Institute are working under the authority of the newly created Bureau for Homeland Security headed by former Governor of Pennsylvania, Thomas J. Ridge, who is reporting directly to US President.

About terrorist involvement in the stock markets via the networks

In this connection, experts assess that world markets probe unusual trading in the days before terrorists crashed hijacked United Airlines and American Airlines jets into the Center's Twin Towers and the Pentagon on September 11. Securities regulators in the US, Germany, Japan and Hong Kong say they are investigating whether terrorists raised money through insider trading on knowledge of attacks that led to the collapse of New York's Trade Center and closed the US stock markets for four days. Investigations may thus lead to those guilty of the terror attacks against the US and show connections with Osama bin Laden.

According to data quoted by Bloomberg, trading in so-called put options, which profit when stock prices slump, involving airline carriers UAL Corp. and AMR Corp., surged in the pre-attack days. "We have heard those reports about terrorist involvement in our markets", US Securities and Exchange Commission Chairman Harvey Pitt stated. "Our division has been looking into a variety of market actions that could be linked to these terrible acts, including the subjects of the rumors", he added. Stock of Morgan Stanley Dean Witter and Co., which occupied 22 floors of the 1 World Trade Center building, and Merrill Lynch and Co., with headquarter near the Towers, also experienced pre-attack option trading of 12 times to more than 25 times the usual volume in put options.

The US Federal Reserve on Monday October 1st, 2001 cut 0.55 per cent off reference rates, for the ninth time this year. Consequently, FED rates went down to 2.5 per cent, their lowest level for the past forty years. More interest cuts for the near future are heralded by the American Central Bank.

It is not very sure about the way this new decision will be received by the consumers, who are the target and the key to any economic revival. This interest rates cut can boost both the volume of population expenses and the level of corporate investments, but it is not clear if the cut is enough to offset the impact of the terror attacks. "The terrorist attacks widened the degree of uncertainty in an economy that was already weakened. Business and consumption expenses will be boosted by a new cut in interest rates", the FED said, explaining its last decision.

One can think that "the perspective of military attacks, the diminished profitability and the almost inexistent economic growth are casting a shadow on the FED intervention. There is no trust in the economy right now, and, until this feeling is

reinstated, the markets will keep fighting for survival", estimated Erik Gustafson, fund manager at Stein Roe & Farnham.

It is very positive that, despite the fact that, immediately after the announcement made by FED, the US market dropped, but made a spectacular comeback afterwards, posting strong gains until closing time. The Dow Jones Industrial Average index soared at 8,950.59, S & P 500 (*Standard and Poor's*) index closed at 1,051.33, up 1.23 percent, while the composite index Nasdaq went up 0.8 per cent, up to 1,492.33 points. The volume of traded shares was quite high, without reaching nevertheless the levels registered in the wake of the terrorist attacks. Significant increases were posted by shares of airlines and defense companies, considering the possibility of US retaliation, which finally was the case. But, on the other hand, shares of the technology companies were affected by revised estimation regarding Q3 financial results announced by Compaq Computer Corp., the world's second-largest computer maker.[22]

Actions combating fraudulent cyberspace users

The behavior towards those who are trying to benefit of the cyber infrastructure of the world, in a terrorist way, was expressed by the US president G.W. Bush, who said: "We are not deceived by their pretenses to piety. We have seen their kind before. They are the heirs of all murderous ideologies of twentieth century. By sacrificing human life to serve their radical visions – by abandoning every value except the will of power – they follow in the path of fascism, and Nazism, and totalitarianism. And they will follow that path all the way, to where it ends: in history's unmarked grave of discarded lies". And he continued: "We know there are struggles ahead, and danger to face. But this country will define our times, not be defined by them. As long as the United States of America is determined and strong, this will not be an age of terror; this will be an age of liberty, here and across the world".[23]

In this respect, the NATO Charter reflects best the attitude of the world: an attack on one is an attack on all. In response to the September 11 attacks against the United States, the NATO Allies, determined to play their part in combating terrorism, have agreed to a package of measures, including, inter alia, enhanced intelligence sharing and co-operation; assistance to Allies and other states which are, or may be, subject to increased terrorist increased as a result of their support for the campaign against terrorism; measures to provide increased security for the facilities of the United States and other Allies on their territory.

As far as OSCE is concerned, in December 2001, in Bucharest, at the Ninth Meeting of the OSCE Ministerial Council, its participating States have adopted "Decision No. 1 – Combating terrorism", According to this decision, the OSCE participating States pledge to reinforce and develop bilateral and multilateral co-operation within the OSCE, with the United Nations and with other international and regional organizations in order to combat terrorism in all its forms and manifestations, wherever and by whomever committed. The decision proclaims the OSCE determination, as a regional arrangement under Chapter VII of the Charter of the United Nations, to contribute to the fulfillment of international obligations as enshrined, inter alia, in United Nations Security Council Resolution 1373 (2001), and will act in conformity with the principles of the Charter of the United Nations. Moreover, the OSCE participating States pledge to become parties to all 12 United Nations Conventions and Protocols related to terrorism by December 31, 2002. They also call for a speedy finalization of negotiations for a comprehensive United Nations Convention on International Terrorism.

The Ministerial Council adopted "The Bucharest Plan of Action for Combating Terrorism", which contains more concrete measures in this field. As an example, the OSCE Representative on Freedom of the Media will support, on request, the drafting

of legislation on the abuse of information technology for terrorist purposes, ensuring that such laws are consistent with commitments regarding freedom of expression and free flow of information. Another example, in the framework of the UN Convention on the Suppression of Financing of Terrorism and UNSCR Resolution 1373 (2001), the OSCE participating States will take action to prevent and suppress the financing of terrorism, criminalize the willful provision or collection of funds for terrorist purposes, and freeze terrorist assets, also bearing in mind UNSCR Resolution 1267 (1999). In this respect, they will, in accordance with domestic legislation and obligations under international law, provide early response to requests for information by another participating State and international relevant organizations.

The Bishkek International Conference on Enhancing Security and Stability in Central Asia: Strengthening Comprehensive Efforts to Counter Terrorism (13-14 December 2001), which was co-organized by the UN Office for Drug Control and Crime Prevention (UN ODCCP) and OSCE, adopted a Declaration and a Programme of Action. In the Declaration, the States participants "Emphasize that terrorism is a global problem and that there must be no safe haven for perpetrators of such crimes and their accomplices. It is a complex challenge due to links with transnational organized crime, illicit drugs, trafficking in human being, money laundering, arms trafficking, computer and other high technology crimes as well as other threats, including the proliferation of weapons of mass destruction". The Programme of Action identified, *inter alia*, the following measures:

– "To adopt national anti-money laundering legislation and create corresponding structures, e.g. Financial Intelligence Units, which can be employed to prevent and suppress the financing of terrorism, as well as other relevant crimes. ..."

– "To work toward rapid ratification and implementation of relevant international instruments, including the 1999 UN International Convention for the Suppression of the Financing of Terrorism, and consider implementing the standards of financial accountability and transparency embodied in the Financial Action Task Force (FA TF) 40 Recommendations on Money Laudering and eight Special Recommendations on Terrorist Financing; to take immediate steps in accordance with UN Security Council Resolution 1373 (2001) to block the assets of individuals and entities linked to terrorist financing".

The Standing Committee of the OSCE Parliamentary Assembly, at its meeting in Sintra, Portugal, on October 9, 2001, had tackled the same problems and adopted a Declaration entitled "Security through Solidarity", containing a number of recommendations aimed at fighting terrorism, namely:

– The OSCE participating States are called to agree upon a definition of terrorism and to elaborate on global strategies of a political, economic, social and cultural nature of fighting this phenomenon.

– The establishment of an international network of sub-regional centres for gathering information on terrorist activities and combating them.

– The adoption of appropriate legislation for surveying the lines of financing terrorist activities and, also, for combating commercial activities, which, even if carried in a legal framework, ultimately support terrorist activities.

– The adoption of the necessary legal measures to enhance the sharing of information and co-operation among the intelligence, security and police services of the OSCE participating States and consider the establishment of rapid reaction forces.

This permanent Panel also welcomed the initiative taken by the Romanian Chairmanship in Office of the OSCE, in 2001, to develop an OSCE wide plan of action for the fight against terrorism.

The United Nations is the framework for the global fight against terrorism. United Nations Security Council Resolutions above-mentioned – 1267 (1999), 1269 (1999), 1368 (2001), 1373 (2001), 1376 (2001) – along with the 12 relevant Conventions and Protocols on anti-terrorism issues, provide the basis for this framework and include a

number of specific elements of combating terrorism. For instance, the Resolution 1373 requires very clearly that every United Nations Member State has a responsibility to crack down on terrorist financing. That means that all Member States must pass the necessary laws to allow the confiscation of terrorists assets. Those laws have to be applied to all financial institutions of every nation. Other international and regional organizations can provide comparative advantages in combating terrorism by addressing various social, economic, political and other factors through all their instruments and structures.

According to the Secretary General, Kofi A. Annan, the United Nations Organization is uniquely positioned to advance this effort. It provides the forum necessary for building a universal coalition and can ensure global legitimacy for the long-term response to terrorism. United Nations conventions already provide a legal framework for many of the steps that must be taken to eradicate terrorism, including the extradition and prosecution of offenders and suppression of money laundering. These conventions must be implemented in full. As the Secretary General Kofi A. Annan has put it, "terrorism threatens every society. As the world takes action against it, we have all been reminded of the need to address the conditions that permit the growth of such hatred and depravity. We must confront violence, bigotry and hatred even more resolutely. The United Nations' work must continue as we address the ills of conflict, ignorance, poverty and disease. Doing so will not remove every source of hatred or prevent every act of violence. There are those who will kill even if every injustice is ended. But if the world can show that it will carry on, that it will persevere in creating a stronger, more just, more benevolent and more genuine international community across all lines of religion and race, then terrorism will have failed".[24]

The democratic world can defeat a network of terrorist cells and bases, even more groups and such networks, but it should be quite clear that terrorism as such will be defeated only when its profound causes and roots are eradicated. It is a much more difficult war, which will be won only when all countries combine their strengths to eradicate those causes and roots. They have to be addressed by an expanding global coalition of the whole world in the framework of the United Nations. Otherwise, there is the risk that the wide attention previously given by many Governments and international organizations to human rights and other social issues would somewhat fade into the background with the enormous challenges stemming from common fight against terrorists acts. One should not forget that these challenges are also stimulating the increased role of the State in some areas of private economy linked to monitoring and control in security matters.

That is not the purpose of this paper to address the causes and roots of the terrorism, which are quite many and very profound. Long centuries of foreign domination and oppression, and some less bright sides of current accelerated globalization can provide some food for thoughts.[25] But one of them is linked to despair and poverty. In this respect, the G7 Statement in Okinawa, 21st July 2000, has underlined that: "The International Development Goal of cutting in half by 2015 the proportion of the world's population living in extreme poverty is an ambitious one. It demands a strategy of ll economic growth accompanied by the right social sector policies, which can contribute to; a virtuous circle of poverty reduction and economic development. Debt relief for Heavily Indebted Poor Countries (HIPCs) is only one part of such a strategy, but it is a crucial part".[26]

Improving the international law

The increased military and economic reliance on information systems introduces new vulnerabilities not adequately protected by traditional kinetic force arms. As a matter

of fact, the international law does not provide appropriate response mechanisms for the States in case of computer network attack.

In international law, an important domain is missing, that of the information warfare, as part of the terrorist or aggressive acts. Obviously, the 12 relevant UN Conventions and Protocols cover a large area of anti-terrorism, but not all of them, and not specifically actions against information warfare. In this respect, the responsibility of the States to share intelligence and coordinate the efforts of law enforcement is a very high one.

Indeed, for the time being, there is no international law protecting network. Some bilateral agreements or specific guidelines have emerged as precursors to unified international law.

A US military man advanced the idea of a functional outline for an international convention, the International Regime for Information Security (IRIS).[27]

In the new landscape, such an Idea deserves a particular attention with a view to be embodied in the existing norms and procedures or in a new international convention on information security under the UN aegis.

It is hoped that all these aspects will be considered in the forthcoming negotiations at the UN on a comprehensive convention against terrorism. An action in this field is a very urgent one and should be an item of high concern and priority of the United Nations and Specialized Agencies.

The General Assembly UN Session, in 2001, which started later, in November, instead of September, because of the terrorist attacks in New York and Washington, has given a serious impetus to the negotiations on a binding convention. It seems that the time for action in this area of challenges has now arrived. In such a way, the new economy will be better protected and will provide fewer threats to security.[28]

---

[1] Wolfgang Munchau, "Some hard truths about the New Economy", in *Financial Times*, Monday, December 4, 2000.

[2] G8, *Okinawa Charter* 01/ *Global Information Society*, July 2000.

[3] Will Hutton and John Knell, "Free spirits usher in network economy", in *Financial Times*, Friday, July 28, 2000.

[4] *The American Workplace: Skills, Compensation and Employee Involvement*, edited by C. Ichniowski et al., Cambridge University Press, 2000.

[5] Robert Taylor, "Skills without frontiers", in *Financial Times*, Friday, April 28, 2000.

[6] Jason Forsythe, "The Great Equalizers: Internet and Education", in *International Herald Tribune*, Wednesday, November 29, 2000.

[7] Kochiro Matsuura, "Hard lessons for world's educators", in *Financial Times*, Thursday, April 27, 2000.

[8] Richard Waters, "Wringing new potential out of the old economy", in *Financial Times*, Wednesday, April 19, 2000.

[9] Paul Taylor, "Reshaping the global landscape of IT", in *Financial Times*, Wednesday, February 2, 2000.

[10] Fiona Harvey, "A race to feed the web's voracious appetite", in *Financial Times*, Thursday, December 7, 2000.

[11] George Cole, "Net spreads by word of mouth", in *Financial Times*, Wednesday, April 12, 2000.

[12] Rod Newing, "Why the internet will become the next mass medium", in *Financial Times*, Wednesday, March 15, 2000.

[13] Wolfgang Munchau, *op. cit.*

[14] Wolfgang Munchau, *ibidem*; European Commission. *The Economy, 2000.*

[15] Peter Norman, "EU leaders agree sweeping reforms to create jobs", in *Financial Times*, March 25/March 26, 2000.

[16] G8 Okinawa Charter, *op. cit.*

[17] Gwen Robinson, "FBI chief urges laws to curb cyber-crime", in *Financial Times*, Wednesday, March 29, 2000.

[18] John Labate, "'Cyber-leaks' threat to corporate secrets", in *Financial Times*, Tuesday, January 25, 2000.

[19] Karl J. Shawhan, Major, USAF, *Vital Interests, Virtual Threats*, Air University Press, p. 25.

[20] Răzvan Scăeşteanu, "Ciberterorismul, mai periculos decât rachetele balistice", in *România Liberă*, 27 octombrie 2000.
[21] *Adevărul*, 17 octombrie 2001.
[22] Bogdan Neagu, "Federal Reserve cuts rates to revive economy", in *Ziarul Financiar*, 4 octombrie, 2001.
[23] George W. Bush, *Address to Joint Session of Congress*, September 2001; US Department of State, *The National Security Strategy of the United States of America*, The White House, September 2002.
[24] OSCE, The Ninth Meeting of the Ministerial Council (Bucharest, December 3-4, 2001), *Decision No.1 – Combating Terrorism, The Bucharest Plan of Action for Combating Terrorism*; The Bishkek International Conference on Enhancing Security and Stability in Central Asia: Strengthening Comprehensive Efforts to Counter Terrorism, Plan of Action; Kofi A. Annan, "Fighting Terrorism on a Global Front", in *New York Times*, Friday, 21 September, 2001.
[25] Valeriu Tudor, "War in the Balkans: Lessons and Challenges Ahead", in *Romanian Journal of International Affairs*, Bucharest, Volume VI, 1-2/2000; "Globalization and its Regional and Subregional Pillars", in *Romanian Journal of International Affairs*, Bucharest, Volume IV, Special Issue Two 1998; *Mondializarea şi Interesul Naţional*, comunicare la Conferinţa Naţională de Cibernetică, ediţia a IX-a, Bucureşti, 7-8 noiembrie 2000 (*Globalization versus National Interest*, paper presented at the National Conference on Cybernetics, IXth Edition, Bucharest, November 7-8, 2000); "The Concept of Democratic Security – Hopes and Realities", in *Romanian Journal of International Affairs*, Bucharest, Volume II, Supplement, 1996.
[26] G 7 *Statement*, Okinawa, July 2000.
[27] Karl J. Shawhan, *op. cit.*
[28] Valeriu Tudor, "The New Economy: New Challenges To Security", in *Romanian Journal of International Affairs*, Bucharest, Volume VIII, 1-2/2002.