Cyberpower and Global Cyberattacks: is cybersecurity possible? Towards a renewed vision and strategy for international security

Professor Solange Ghernaouti, Swiss Cybersecurity Advisory and Research Group, University of Lausanne, Switzerland, *sgh@unil.ch*

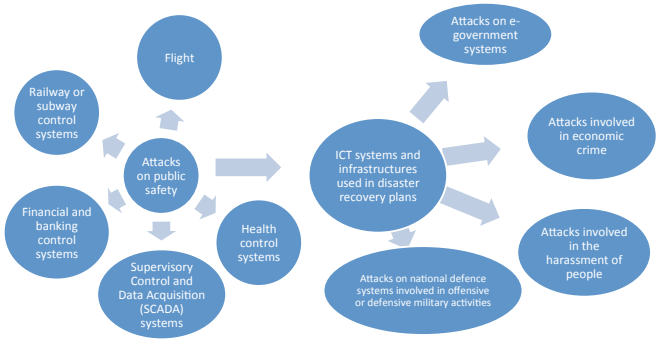
***Abstract*— The term "cyberattack" is being widely employed nowadays in a variety of contexts. This paper discusses the nature of the activities that commonly find themselves included under this term, identifies their distinctive features, their technological components, impacts and motivations, and seek to distinguish between their military and civilian aspects, insofar as this is possible given the interconnectedness of applications and infrastructures, military staff, civilians and experts for hire. The questions of risks and responses are then considered, along with the implications of the quantities of data that circulate, often without the knowledge or the approve of the individuals concerned, and discuss the requirements for and possible forms of cybersecurity strategies, approaches and measures that will protect individuals, organisations and states, and provide appropriate frameworks of control while at the same time preserving essential civil liberties and human rights. In particular the role and necessity of implementing appropriate public-private partnerships at national and international levels will be considered, along with the possible strategy of designing an international treaty that will improve legal mechanisms dedicated to mastering cyber-risks and to improving the efficiency of the fight against global cyber-incidents.**

***Index Terms*—Cyberwarfare, cyberattacks, security, control, society**

I. INTRODUCTION - THE VARIOUS LEVELS OF IMPACT OF CYBERATTACKS

THE term "cyberattack" can have several meanings, depending on the targets, the victims and the motivations of the perpetrators, and the scope, the impacts and the consequences of the attacks. Some have minor impacts and can often be attributed to straightforward delinquency, while others could have drastically negative effects on people, organizations and states, and could be linked to crime, to terrorism or to war (Figure1).

Because of the multiple interdependencies of ICT infrastructures, it is essential when considering the impacts of cyberattacks not to limit the analysis to one single perspective. These attacks could have several separate or domino effects, and human life could be endangered even if the cyberattack is not innately designed to do so. It is always difficult to identify such dependencies precisely in order to be able to control potential collateral damage, to understand the long-term effects, or to prevent the dramatic socioeconomic effects of cyberattacks.



1

Fig 1- Different kinds of targets of cyberattacks

Very often the use of the word "cyberattack" instead of "cybercrime" can indicate that the attacks were directed against the computer and telecommunication systems involved in vital infrastructures that have a serious role to play in the economy, the safety of people, the sovereignty of a state, and the military and defence systems of a country. These attacks are offensive actions that alter, disrupt, manipulate, degrade, or destroy data, information and communication infrastructures (hardware or software). They could impact the whole of society by destabilising, for example, the efficient operation of the economy or governmental services.

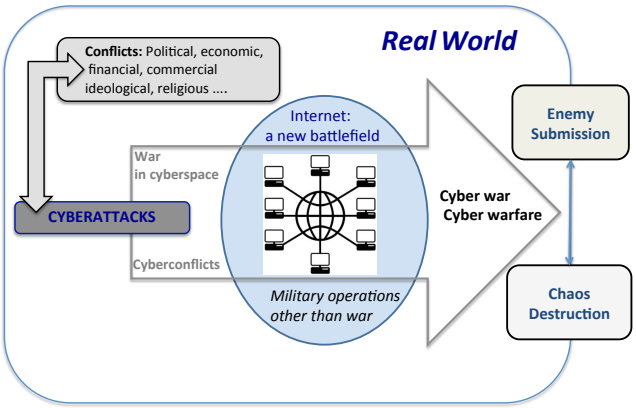
For an attack to be identified and treated as an offensive action that infringes a law, that law by definition must already exist. But cyberattacks exist without any laws to qualify them. The term cyberattack covers a broad range of activities and is

independent of any specific classification of offences.

II. A WORLDWIDE ISSUE: THE EMERGENCE OF NEW PARADIGMS OF WAR AND NEW BATTLEFIELDS

At the same time, the word cyberattack can also be understood as referring to a military technique. ICT infrastructures, information/disinformation procedures and cyberattack-related tools are increasingly being linked to war-making capacities that contribute to developing the potential for cyberwarfare.

Cyberconflict is a generic term that defines cyberattacks resulting from retaliatory actions between nation-states or organised groups as a response to contentious or conflict situations. When states themselves carry out cyberattacks within a military context, the term cyberwar is preferred (Figure 2).



2

Fig. 2 – Cyberconflict and war in cyberspace (Adapted from S. Ghernaouti, Cybercrime, Cyberconflict, Cybersecurity and Cyberpower, EPFL Press 2012)

The term "cyberwar" should nevertheless be used with caution, and only when cyberattacks are related to military personnel who are targeting systems operated by enemies and located in foreign countries. At present an amalgam of terms and concepts is in common usage, a situation largely supported by the media and by cybersecurity product and service providers; this has led to confusion and contributed to the development of fear of a phenomenon that is fluid and difficult to qualify. At this moment there have been no real cyberattacks of a purely military nature in the classical sense of the term, and thus it is surely preferable to refer to cyberattacks linked to cyberwarfare rather than cyberwar. This subject will be addressed again in Section IV below.

It is true, however, that cyberspace has progressively become a political and a economical battlefield; where cyberweapons (malware, hacking, DDoS, …) can potentially target, entirely indiscriminately, civilian ICT resources as well as cyber-based military systems. To some extent the Internet could be seen as a weapon of mass destruction, insofar as a program that could serve as an enemy, a spy or a thief could be installed in any piece of electronic equipment. This is particularly true when considering, for example, the capabilities of malware for propagation and infection, the number of existing botnets and zombie servers that could be involved in a distributed denial of service attack, or the way that a country, a region, or even a continent could be cut off from the Internet.

Because of the multiple dependences and interdependencies between critical infrastructures, it is sometimes difficult to make the distinction between military and civil domains. Some cybersystems can belong to military bodies but be accessible through infrastructures useful for supporting the needs of the civilian sector. This is particularly true, for example, when considering systems for the production and distribution of electricity. In the same way, many vital infrastructures and services are dual use or have primarily been built to support the needs of the civilian sector. Moreover, civilian ICT infrastructures can be important to the military sector to one degree or another and targeted by potential cyber attacks. If so, it could be difficult to qualify such a cyberattack as an act of war on the basis of its impact, as very often the source of the attack is not clear and the attack can be performed from multiple sources or by passing through several systems, network or countries. International cyberattacks can be performed though proxy systems and infrastructures making the origin, the initiator, and the organizer difficult to determine, and equally making it difficult to demonstrate that a particular government or agency was behind it.

III. NEW THREATS AND RISKS IN A NET-CENTRIC WORLD

New kinds of threats have emerged in cyberspace that affect and implicate both the civilian and military domains. Facing up to cyberattacks, whatever their aims and motivations, requires rethinking security and adapting military doctrines and defensive mechanisms. Identifying and understanding these new cyberthreats are important in developing effective cybersecurity measures and military cybercommand capabilities. The more developed a state is, the more its military capacities and economic power are dependent on Information and Communication Technologies. They are then weakened because they are more vulnerable to major computing attacks.

It should be remembered that security incidents related to natural catastrophes, errors and failures and ICT damage caused by human behaviour or misuses (including criminal and terrorist acts), and the intensification and the increasing complexity and efficiency of cyberattacks are problematic at several levels of society.

Not every cybercriminal action is an example of terrorism or war between states. However, the Internet introduces new risks for states because it can become a weapon. The Internet can support a political project and be used in a situation of conflict, or even to harm an enemy without fighting, by reducing the enemy's power in economic, scientific or cultural domains. No country is shielded against cyberactions aiming to harm it.

In a net-centric world, the Internet allows the use of indirect strategies that even in peaceful times can contribute to weakening a business sector, an enterprise or a country, and thus generate competitive advantages to some socio-politico-economic players. The high stakes in play over controlling space, communications satellites and GPS technologies are additional examples that illustrate the intense competition between states in the field of information technologies. Cyberspace is an ICT environment that countries have to master to ensure the smooth functioning of the state, even in peacetime.

IV. Cyber-aggression

Among the most significant computing attacks can be found attacks that target a nation's critical infrastructure and of which the consequences are harmful to society within, and the national security of, that country. If the financers of such attacks are states, these attacks can be considered as part of a military strategy encompassing intimidation, retaliation or offensive computing. When associated with or carried out alongside more classical military activities, such offensive computing attacks can neutralize an enemy's defences, destabilize its intelligence services, contribute to altering its decision-making process, mislead the enemy, paralyze strategic centres, or even block means of communication.

The term "cyberwar" is often misused because of its importance. Some DDoS attacks against governmental or commercial websites have been misreported in the press as acts of cyberwarfare. The term cyberwar should be used with caution because there is not yet any clear, consensual, universal definition of what constitutes an act of cyberwar. Does a specific attack aimed at defacing a governmental website constitute an act of war? Can this be compared to a cyberattack on the systems that controlling a nuclear power plant? Do cyberattacks need to accompany real military acts? Can a cyber-aggression be attributed clearly to a state, even if civilians perform it? Is a piece of malware comparable to an anti-personnel mine?

The notion of offensive operations used to distinguish acts of war is usually tied in to the number of casualties and the amount of destruction caused. Thus the jamming of communications and cyberattacks on air control systems or on production facilities for essential products, such as chemicals, for example, could be considered to be acts of war. When such attacks are carried out, populations could potentially be just as affected as in the bombing of Hiroshima or in other actual conflicts.

The remote control of computers, if performed or financed by the military (the notion of military botnets), can be viewed as being similar to infiltrating remote-controlled soldiers. On this basis, hacking can be considered as a weapon of war and making distinctions between the civilian and the military becomes even more difficult.

If major, massive attack scenarios are plausible, full-scale attempts have not yet been made. The existence of the dissuasive force that states possess at an international level is analogous to the nuclear deterrent. This analogy is certainly exaggerated but the principle remains: there is a large number of states with the potential capacity to launch massive cyber-attacks or counter-attack. It would be a mistake to underestimate the potential of cyberthreats in a government's interactions, alliances, games and geostrategic equilibriums. At the same time, however, the total destruction of the Internet through attacking the "root" servers, for example, is not conceivable because there is a real international will to prevent a massive cyberwar and to ensure the survival of the Internet, because its destruction would not be beneficial to anyone.

Usually crime-related issues and military issues are handled and studied separately by specialists in civil or military matters. Crime is a legal problem related to law enforcement and the justice and police systems, while war has traditionally been a subject for military staff and specific governmental agencies. Nowadays, however, as we have seen, cybercrime and cyberwarfare are carried out using the same kind of tools, know-how and technical infrastructures. Cyberwarfare uses the same toolkits (malicious software, technical exploits) as those developed, used and made available by cybercriminals in underground markets. Because cyber-mercenaries exist in the marketplace and perform whatever is lucrative for them as a job, non-state actors can be involved in both cybercrime and cyberwar. The evolution of cyberattacks over the last decade is evidence of the abolition of frontiers between cybercrime and cyberwar. To cite only one example, the Conflicker Worm, since its discovery in 2008, has infected government sites, military networks and home computers all around the world. Several releases exist that have facilitated the propagation and infiltration of this worm.

Considering ICT as a weapon for offensive and defensive strategies remains a necessity, however, and any military doctrine should include such considerations. Most frequently, specific resources are dedicated to cyber-warfare, from strategic, tactic and operational points of view.

ICT could lead to major disruptions and problems. In addition, it could add to the problems of new risks related to:

- ICT robustness, dependability and reliability;

- ICT dependencies;
- ICT supply chain;
- Confidence in ICTs manufactured in other states that could potentially be enemies of a nation.

The ability to achieve victory depends on the control of information and its environment, including human and technological support. ICTs are areas of innovation in waging war that provide the opportunities to launch different kinds of attacks, to surprise enemies or to adapt strategies and positions when confronted with an enemy that also controls information.

ICTs also lead to war in cyberspace, using information systems, software and data. Purely military skills are replaced by political, security, IT and criminal skills. The number of combatants can be reduced as front-line soldiers are replaced by specialised teams (the notion of cyber-forces). There are no more direct confrontations and no need to physically cross geographical borders in order to invade a country.

In the same way as the air, the sea and the land, cyberspace is now a domain where military actions can take place, with the motivation of forcing the enemy to fight on a terrain for which it is not ready, not equipped or not prepared. White-collar war exists in the same way as white-collar crime. A war in cyberspace might appear at first glance to be cleaner than a real war. But cyberwars are more hypocritical, in some sense, and more indirect (they allow the avoidance of direct confrontation); they can employ various intermediaries (technical, human and geographical); and they can have effects that are not immediately and visibly apparent and are thus more difficult to attribute to specific causes. Cyberwars can be very efficient and have impacts at different levels, such as economics, ecology, technology, media and psychology. The use of electromagnetic impulse weapons that can prevent information processing and telecommunications in a rapid and definitive way (the notion of technological destruction) can be as harmful and effective as the use of chemical, biological or even nuclear weapons, to the extent that all human activities have an increasing dependence on information technologies.

V. Responding to cyber acts of war

It is nearly always difficult to identify the persons responsible for launching cyberattacks, be these politically or criminally motivated, unless the authors actually claim responsibility. This latter situation is often the case with terrorist attacks. The perpetrators want to attract or gain visibility to enhance the impact of their actions and present their claims. At the opposite end of the spectrum, criminals prefer discretion. In political conflicts the ambiguity and uncertainty related to cyberattacks are often preferred. If a state can avoid the possibility of the clear attribution of responsibility for cyberattacks to their agents, this makes it difficult for the country that was attacked to retaliate in an aggressive way, be it a physical or electronic response. Cyberattacks should have “sufficient gravity” to be considered as armed attacks.

The question of the attribution of responsibility is a crucial one and a major issue for the international community in that it raises several legal questions. One current debate concerns whether cyberattacks are essentially a criminal matter, and thus subject to domestic criminal law, or acts of war to which international laws on warfare should be applied [1]. The Rules of War require the attribution of an armed attack to a foreign government before responding with force.

The point is the determination of whether the country that has been attacked has the right to respond to an act of cyberwar, either using only passive defences or employing active cyberdefence measures against the ICT infrastructures of the other state. This could includes the right to use cyberattack countermeasures not only against the state at the origin of the cyberattacks but also against some or all of the intermediary states that had passively allowed, or contributed to, the attacks and had neglected, knowingly or not, to prevent cyberattacks from within their national borders. Sometimes active defence could be viewed as a form of reprisal and be used as self-defence in anticipation of a real attack.

As yet there is no international treaty, convention or protocol that addresses this question or the question of how to distinguish a criminal cyberattack from a military cyberattack. Individual states are thus free to interpret their rights on the basis of their own legal corpus and culture, taking into account guidance from existing international laws and the means on which states have long relied to solve their disputes peacefully. If it were determined that only criminal laws should apply, that would mean that the countries would not have the right to use active defence and thus their defences would rely solely upon their capacity to prevent and deter cyberattacks (passive defence). From the perspective of military doctrine this is insufficient, especially given that cybercriminals can act with impunity from the shelter of digital paradises and that some countries are not sufficiently active in respect of the prosecution or extradition of cybercriminals. Deterrence based on criminal law also raises the problem of the effectiveness of both law enforcement and international cooperation when dealing with international cyber-attacks. Within their national territory, states should prevent (and not encourage) the perpetration of cyber acts of war against other territories and refrain from providing any form of support to individuals to commit such acts, if the state wishes to avoid the risk of being held (indirectly) responsible for such acts. The same principle applies of course to the state’s attitude towards cybercrimes.

VI. Cybercrime, cyberhostility or cyberconflict?

Both public and private companies often risk having their resources and information stolen and their communication

networks penetrated. They also run the risk of being the victims of hackers, sometimes as part of coordinated attacks on sensitive infrastructures. These risks must be taken seriously as potential threats to competitiveness, reputation, and, to a larger extent, to state sovereignty, national or public security, or even democracy itself.

As a result of the opportunities available for carrying out cyberattacks, and the expected growth in the scope and sophistication and consequences of these attacks, cyberspace should be considered as a risky domain for all of its users. As we have seen, the risks concern not only nation-states, but also all private and public organisations and individuals. Because of the high correlation between the political, economic and social stakes and challenges in real life and in cyberspace, and the huge economic competition that exists in a interconnected and globalized world, state-level cyberthreats, cyberattacks or cyberhostilities can be a tactic to develop supremacies and hegemonies or to dispute cyberterritories. Such activities could contribute to controlling enemies (economic or political) in a kind of "Cyber Cold War". Although it seems unlikely that a real cyberwar is ongoing, this does not mean that a new spiral of cyberactivities is not emerging.

States have to develop and enforce the robustness and resilience of ICT infrastructures and, at the same time, need to enhance their means of anticipating and preventing cyber attacks and develop means of (potentially) attacking their enemies. From now on, cyberattacks and cyber counter-measures will be part of national defence systems and military doctrine. These include all forms of passive cyberattacks, such as espionage and intelligence information gathering, and are not limited to offensive and destructive cyberattacks.

VII. Towards an Untrusted Cyberworld and an Era of Hypersurveillance

The Internet, a source of knowledge, of culture and of exchanges is also a source of disinformation and propaganda, easy to produce for the same reasons as the truth is easy to publish. All the necessary tools are easily available: software to re-touch photographs, software for editing documents, scanners and formatting tools. The Internet allows the transmission of rumours, urban legends, false accusations and simple lies with particular ease because there is no right to forget and because of the fascination created by the media often leads to a lack of common sense on the part of the Internet user, who is ready to believe whatever it is that he is looking to hear. In the absence of a trusted third party, everyone chooses the identity they want: perfect for playing or teasing, impressive for cheating or corrupting. The twelve-year-old girl is actually a habitual paedophile (exploiting this kind of false identity for nefarious purposes is known as grooming). The supposedly trustworthy banking site is actually a fake site designed to acquire the identities and credit card details of Internet users who have been tricked (this is phishing). The brilliant company director and the beautiful but lonely foreign lady are in fact crooks who make contact in order to pick up a few thousand Euros through seduction or playing the charity card…

As a medium based on anonymity and thus a dream tool for criminals and terrorists, the Internet can also be used for propaganda, proselytising, and remote and discreet exchanges. What is a drugs network or a separatist of ideological organisation if not a hierarchical grouping of correspondents scattered around the world who use new technologies for their own purposes? States, public authorities that rely on their intelligence services and judicial systems, all need to be able to explore, monitor, control and even restrict the use of the Net.

In parallel we are seeing the development of tools for searching, for social engineering and for business intelligence that are digging ever deeper into the Internet, crawling around and bringing to the surface, in a structured way, a huge quantity of information, the merging and cross-referencing of which is shaking the long-established rules of privacy and private lives. Soon, more information will be available in open sources than in police files. This is already the case for honest people, about whom state services in reality actually know little, and far less in any case than large businesses actually do.

How can we not be reminded at this juncture of the chilling phrase attributed to Felix Dzerzhinsky, the founder of the Soviet KGB: "the only ones who fear surveillance are those with something to hide". A phrase that returns now to explain that, contrary to what was the rule for a very long time, every citizen is now fundamentally viewed as a suspect. Thus as hyper-surveillance is little by little imposed upon us, both authorities and commercial entities, in particular with the help of social platforms, try to convince us that we are all under threat from "the others", that "the other" is both an enemy and the object of permanent curiosity, and that for our own safety and security we need to be totally transparent.

Recent rapid and wide-reaching advantages in technology and in our use of, and dependence on, these technologies, have contributed hugely to the phenomenon by which individuals can find themselves tracked and monitored to a degree never before thought possible, using data that they themselves provide. Smartphones and mobile Internet use, RFID and geotagging, logging into social networks and using local resources, all of these activities and technologies allow an unprecedented level of geolocalisation. The data are out there, even if the task of processing and using these data is non-trivial, to allow movements, activities and contacts to be monitored as never before. It can rightly be remarked that the Era of Information is being transformed by the digital traces we are leaving behind us into an Era of Hypersurveillance.

It is also worth bearing in mind the kind of information that is circulating around all of us, our digital ecosystem. Any person who has even the slightest presence on the Internet can

soon begin to identify information, provided willingly or unwillingly, by themselves or by others.

It is a question for all of us, how much of this information we wish to make public, knowing that as a general principle once information is out on the net it cannot be recovered and removed. The network never forgets.

So what are the perspectives for the future and what are the stakes in play?

Inevitably when considering the quantities of information available, the means of generating, storing and analysing the data, and the uses to which all this information might be put, questions of control arise. Both control of the information, and control by authorities and less legitimate entities of the movements of individuals and material.

The next major question that arises concerns the right to secrecy, to privacy, to self-determination, to autonomy and to freedom. When so much information is widely available about individuals and groups, how can these individuals ensure that it is not used and abused, forcing them into certain behaviours or encouraging them to act in ways that are not to their own ultimate benefit?

The explosion in the use of these technologies and of the quantities of data generated and analysed is visibly leading towards some kind of technological arms race, where behaviours and attitudes are evolving and being driven by the technologies on offer and the uses to which they are being put. Ever faster, ever more functional, ever more pervasive; no end is in sight for the collection, analysis and application of these data.

Perhaps the most significant development over recent years has been the move towards the expectation of permanent connectivity. Even twenty years ago net access was fleeting and slow, based on dial-up connections that hogged the telephone lines. Nowadays, this has been forgotten as permanent access through wifi networks and data subscriptions for smartphones are becoming ubiquitous.

In summary, then, we can note the wise words of La Rochefoucauld writing nearly five hundred years ago, who remarked that when we lose control over our own secrets, we lose a key element of our freedom to think and act as we wish. Essentially we become dependent for our integrity and security on those to whom we have confided our secrets.

In a context where we are all increasingly providing large quantities of personal information to the service providers we use and the people with whom we interact on a daily basis, we should all be attentive to the potential impact of the gathering and analysis of these data and the uses to which they may be put.

VIII. Solving the impossible equation, or the paradox of liberty[1]

A compromise is required, a compromise by which cyberspace is guaranteed to be both free and protected, secure so that every user can freely exercise his basic rights without hindrance, a place for exchanges, of knowledge, of culture, of pleasure and of business that is sheltered from the Big Brother gaze of governmental, intergovernmental, commercial or criminal groups. A space where one behaves according to codified rules, recognised by everyone except the criminal fraternity, with territorial and extra-territorial zones that are clearly defined and subject to arbitration and recognised international authorities that are recognised by all. If we consider Article 28 of the Universal Declaration of human Rights: “Everyone is entitled to a social and international order in which the rights and freedoms set forth in this Declaration can be fully realized”, in what way is cyberspace different in that this order should not apply? What else can be done, in a world that is now subject to the law of information and communication technologies and an international treaty on cyberspace, if not the implementation of the last two paragraphs of Article 29 of this Declaration, for example? [2]

The UN already possesses, in its founding charter of 26 June 1945, a tool for controlling and administrating international conflicts that can be applied by extension to cyberspace. Chapter VII: “Action with Respect to Threats to the Peace, Breaches of the Peace and Acts of Aggression [3] is relevant to current times and can be easily applied to cyberconflicts. Let us imagine – as an example – a denial of service attack by one country on another, aiming to block its governmental communications or trade exchanges. The application of Articles 41 [4] and 42 [5] is just as legitimate as in the case of a more traditional military attack.

The military aspects, so frequently at the centre of the debate around cyberspace – for the same reasons as games and the sex trade are the catalysts for the development of the media – have allowed the creation of areas of research that have rapidly been identified and worked through. The correct ordering of all the domains – civil, penal, commercial, legal, cultural – can only be envisaged in the framework of an international treaty.

IX. The need for innovative approaches to cybersecurity

Without yielding to the ideology of fear, the fear of ecological risk, the fear relating to public order, it is essential that a real public debate takes place, not only around questions

[1] This paragraph is an English translation and adaptation of the following French publication “Le cyberespace: une valeur commune à protéger” S. Ghernaouti-Hélie; C. Aghroum. Rapport de l’Observatoire national de la délinquance et des réponses pénales 2011. CNRS Editions (www.cnrseditions.fr)

of the increasing reliance of society on information and information systems, but also on the related subjects of the security of citizens, of organisations and of states, all within a world of generalised interconnections. Cybersecurity must be understood both in a context of a global society and in a holistic way that will permit finding a realistic balance between the needs for, and requirements of, protection, between the assurance of individual and collective interests, and between the sovereignty of individual states and the needs for international collaboration, all the while respecting the fundamental rights of all humans. These points should logically form a privileged basis for the development of a connected information society.

The major players on the Internet, both public and private entities, have a duty to develop and offer security solutions that address technical, legal and financial issues and are both realistic and convincing, solutions that mean that liberties are not exchanged for an illusion of security and that when necessary the work of the justice system and the police can be effective without damaging fundamental liberties.

These security solutions should not lead people to forget that such measures alone cannot protect against injustice. It is essentially a piece of deception to make people believe in a technological and security-based mirage, to promote as an unquestionable asset obligatory and generalised surveillance, and to train consumers and those being managed to adopt a docile pattern of behaviour. This final point gives legitimacy to the removal of liberties as soon as no countermeasures exist. The independence of the Group of 29 in Europe [6], is fundamental in this respect.

It is thus essential that reliable and convincing long-term security solutions exist and can be used by the public, so that the situation of exchanging liberties for ineffective protection can be avoided. The idea of being able to protect human rights in respect of technologies and security requirements presupposes the existence and availability of information, debates, realistic alternatives and a real willingness on the part of all of the concerned parties. Beyond simplified ideas of good and evil, between paranoid fantasy and naïve mythology, cybersecurity needs to be developed in a framework of transparency and sincerity.

X. Conclusion – Towards Greater Stability in Cyberspace: A Shared Responsibility

It should not be forgotten that the network of networks, although it is a excellent tool for creating contacts, for developing knowledge, for economic and social development and for personal fulfillment, is also an instrument of power, a commercial zone where everything can be bought and sold, and an infrastructure that allows monitoring and surveillance on a very large scale. Cyberspace is not only virtual; it is an economic and military battlefield and a domain where criminality and terrorism can find outlets. It represents a vision of the world in which political, economic and social realities are reflected.

For the well-being of the digital society in particular and humanity in general, a real political willingness at national and international levels is needed to stop the arms race in cyberspace (or at least to restrict it to an acceptable threshold), and to ensure that cyberspace is not destroyed or altered by unfair practices or by intense competition.

Cyberspace should be considered as an essential, open, global common resource and should benefit from international treaties designed to contribute to reducing accidental or deliberate cyber-incidents and cyber-attacks, regardless of their originators (individuals, recreational hackers, militants, extremists, hacktivists, criminals, militaries, governmental or private institutions). It raises issues of our responsibility (at an individual, national and international level), of international cooperation and of the necessary partnerships between the private and public sectors.

References

[1] *http://www.icrc.org/fre/war-and-law/treaties-customary-law/geneva-conventions/index.jsp*
"Rules of War" refers to several Conventions, Treaty and Protocols. Among these we can quote the following:
- Hague II Convention (1899); Hague IV (1907) : Laws and Customs of War on land
- Geneva Convention (1864): Amelioration of the condition of the wounded on field of battle;
- Geneva Protocol (1928) For the prohibition of the use in war of asphyxiating gas and of bacteriological methods of warfare.

Geneva Convention revised in 1949:
- Geneva Convention I: For the amelioration of the condition of the wounded and sick in armed forces in the field
- Geneva Convention II: For the amelioration of the condition of the wounded, sick and shipwrecked members of armed forces at sea
- Geneva Convention III: Relative to the treatment of prisoners of war
- Geneva Convention IV: Relative to the protection of civilians in time of war
- Geneva Convention (1975): Prohibition of the development, production and stockpiling of bacteriological and toxin weapons and their destruction
- Protocol I (1977): Relating to the protection of victims of international armed conflicts
- Protocol II (1977): Relating to the protection of victims of non-international armed conflicts
- Protocol III (2005): Relating to the adoption of an additional distinctive emblem

[2] *http://www.un.org/en/documents/udhr/index.shtml* "§2. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. §3 These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations."

[3] *http://www.un.org/en/documents/charter/chap7.shtml*

[4] Ibid. "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such

measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."

[5] Ibid. "Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

[6] *http://www.edps.europa.eu/EDPSWEB/edps/lang/en/Cooperation/Art29* "Advisory working party created by Article 29 of Directive 95/46/CE. The Article 29 Working Party is composed of representatives of the national data protection authorities (DPA), the EDPS and the European Commission. This very important platform for cooperation has as its main tasks to:

- Provide expert advice from the national level to the European Commission on data protection matters.
- Promote the uniform application of Directive 95/46 in all Member States of the EU, as well as in Norway, Liechtenstein and Iceland;
- Advise the Commission on any European Community law (so called first pillar), that affects the right to protection of personal data