***Contribution to “La inteligencia económica en un mundo globalizado”, Cuadernos de Estrategia 162, Instituto Español de Estudios Estratégicos, Ministerio de Defensa, Madrid, Junio de 2013***

***LOS RIESGOS ECONÓMICOS DE LA CIBERGUERRA***

**The Economic Risks of Cyberwar**

*March 2013*

*Henning Wegener*

**Abstract**

The increasing acceptance and introduction of digital technologies in military planning and armament opens the perspective of a cyber warfare that, given the global interdependence of net structures, would unavoidably and deeply affect the economy and vital societal assets. Hostile military use of these technologies could, for factual and legal reasons, not be cleanly separated from cyber conflict in general and raises serious questions of controllability and legitimacy, thus opening up highly disturbing damage perspectives. There is the perennial dilemma that the exponential growth and ultra-rapid development of cyber technologies and new sophisticated uses are in conflict with the equally exponential growth and sophistication of attack options. The amazing quantitative and qualitative growth of digital systems and infrastructures in *a second digital revolution* comes accompanied by an equal or even superior growth in attack options and thus in vulnerabilities. Yet, the benefits of the digital age accrue only if there is trust in the functioning, availability, integrity and safety of the underlying technologies: thus, cybersecurity has come to be a global challenge. The article describes actual and possible future cyber developments and the evolving threat landscape in terms of new attack modes, new perpetrators, and new dimensions of economic risk and loss.

The article argues that the deliberate military use of digital technologies in a cyberwar mode should be delegitimized or that at least its offensive component be deemphasized, but that the best course for all stakeholders, including economic actors, would be to optimize strategies for the prevention and mitigation of cyber damage. The key concepts – for all forms of cyber conflict - are self-defense, resilience, security improvements in the IT industry, standard setting including standards for cloud safety, technical redundancies, restraint, national and international cooperation, emergency responses, effective information exchange and warning systems, increased efforts to harmonize cyber penal law and sanctions, advances in international law enforcement, and building international norms of behavior for the cyber age The article concludes emphasizing the need for a universal culture of cybersecurity, and offers an outline of a concept of cyber stability and “cyber peace”.

***Key words***

*Cyberwar, cybersecurity, cyber conflict, cyber attack, cyber infrastructure, critical national infrastructures, new digital technologies, cyber law, threat landscape, resilience, culture of cybersecurity, cyber law, cyber stability, cyber peace*

**I.**

**Cyberwar and Cyber Conflict: the Economic Dimension**

An earlier volume of this series of *Cuadernos de Estrategia,* published inDecember of 2010, concentrated its analysis of cyber threats on the national security dimension[[1]](#footnote-1). The current essay will examine the consequences of cyber insecurity and cyber conflict for economic security and economic intelligence. As the underlying threat factors are the same or similar - and economic security is, after all, an essential ingredient of national security - , the analysis will build on the earlier publication, which remains entirely timely and valid, although some more recent developments and figures have of course been incorporated.

Understood literally, our topic appears to focus on the economic damage that may be inflicted by the hostile use of cyber technologies in a *military* context, thus positing a direct relationship between economy and war.

Indeed, history has shown that war – traditionally conducted with kinetic weapons – has always spelled enormous risks and damage to the economic assets of a belligerent country: by its *indirec*t effects on infrastructure, consumption patterns, economic processes and client relationships, the general functioning of society, etc.; as *unintended,* collateral damage where the effect on strictly military targets spills over into society at large including essential infrastructures, - or *directly*, as part of a deliberate strategy to destroy the economic grid of an enemy country, especially with regard to its armament industry or transport infrastructure, the “war economy”, or beyond, to break the morale of the adversary and to undermine the will of its populations to fight and resist.

Modern war has increasingly engulfed societies as a whole. Its intended comprehensive destructive effect has certainly seen its climax in the Second World War, a “total” war, where the practically unlimited explosive power of weapon systems, including nuclear weapons, and the strategic will of the parties entailed the whole-sale destruction of enemy territory, economic assets, cities and populations included, with new dimensions of violence and human suffering.

When we enter the digital realm, other laws govern. Digital attacks including those with a military purpose are primarily non-violent and relatively low-cost, - “bits instead of bombs”, exclusively by way of electronic invasion of systems and net structures. That also holds for military assets. ITCs, Information and Communication Technologies, have revolutionized military affairs, including battlefield information and communication and weapons systems, but at the same time increased vulnerabilities to such invasions. A cyber attack comes from an invisible enemy, is hard to track and trace, is asymmetric, difficult to assess in its amplitude and final effect, uncertain in the overall damage caused to assets beyond the accountable economic consequences. And while there will be less bloodshed and physical destruction, the consequences could yet be disastrous and touch profoundly on the economy.

Many definitions where authors venture to define cyberwar, describe it as politically motivated actions by a nation state to inflict upon an adversary damage of military relevance -damage to military computer networks, command-and-control systems, air defense networks and “network-centric” weapons systems by digital means[[2]](#footnote-2). More than 100 countries have reputedly established cyber commands and understand cyberspace as the fifth domain of warfare, just as critical to military operations as land, sea, air, and space. More than 30 countries are known to have developed explicit cyberwar doctrines; more than a hundred possess the technical prowess to develop offensive military capabilities. There is a general understanding that cyberwar is a real and portentous military warfare option that has to be taken very seriously, although scenarios and predictions as to its likelihood differ. One concern in this respect is the autonomous growth of cyber commands and cyber war doctrines that may follow traditional military thinking patterns as if afflicted by autism, oblivious of the interconnected cyber context. Thinking in terms of cyber*war* may lead one into a terminological trap. We will return to this worrying aspect.

However, a brief review and juxtaposition of the various available definitions of cyberwar quickly reveals that they clarify little, and that cyberwar remains an elusive concept at best. The naked minimum substratum is that we are dealing with digital attacks on systems and cyber infrastructures. Almost any further definitional criteria are open to doubt or ambivalence. Politically motivated attacks? If espionage, including espionage in armament industries and national infrastructures, is a prominent element in cyber war, as most of the definers claim, political and economic motives are naturally intertwined, and economic gain or data theft may well be the dominant motive[[3]](#footnote-3). Cyber terrorism (a concept to which this analysis will return) certainly has political motives, but does not pursue state-to-state war aims. Action by States and governments? Yes, attacks may be State-run, but the more likely and more effective scenario is that crime consortia, digital mercenaries as it were, are employed to inflict digital havoc at least as auxiliaries, - unholy alliances between rogue States and organized crime as a provider of “crime as a service”. “False flag attacks” could occur when states or non-state actors undertake a cyber attack in the disguise of another state; the resulting misperception could entail consequences that defy imagination, as generally misperception that follows from errors of attribution or wrong interpretation of an innocuous intrusion as a preparation of major attack could be fatal. Ambiguities abound. ¿Military targets? Indeed, should governments lead a determined attack on an enemy country, cyber commands may be spearheading the campaign, military assets will be at the center of any attack, and modern network-centric military systems are sure to be aimed at as preferential targets. Yet, what about comprehensive military and industrial espionage? Even a schematic outline of principal scenarios proves that the spectrum of targets is much wider, and that military planners already include by implication at least critical infrastructures and vital non-military communication systems in their target list, as most of these are dual purpose. All four of the scenarios most frequently mentioned in military-political analysis – the Estonia “cyberwar” in 2007 with its massive attacks on government and important infrastructures by distributed denial of service saturation, the combination of cyber attacks and kinetic means in the Georgia conflict in 2009, the persistent “low level” threat of military espionage, or the hypothetical “all out” cyberwar on defense assets, governments, the economy and infrastructures described in a somewhat sensationalist, but in the last analysis realistic way by Richard A. Clarke[[4]](#footnote-4) - are multi-target, half military, half civilian attacks and show, that cyberwar in its pure definitional form is very difficult to find; the heuristic value of the cyberwar concept is thus very limited, and an *integral assessment* of cyber conflict and cyber threats is by consequence unavoidable. It is exactly such an integral perspective that can demonstrate the tremendous destruction potential of a far-reaching cyber attack. This author is not given to dwelling on dramatic doomsday scenarios, but the extant literature on possible “digital Pearl Harbour” events can neither be disregarded nor trivialized[[5]](#footnote-5).

The key factor that renders any definitional effort to characterize cyber war as a distinct category of hostile behavior so difficult lies in the digital technology itself: the means of attack between civilian and military are identical, almost always dual-use, whatever the motives and targets. Any attack on the now all-pervasive net structures affects (all) digital participants in an unforeseeable and often uncontrollable way. One may regret the absence so far of a systematic investigation on the likely *cascade effects* of even a limited military cyber attack and its international repercussions, which is to say, a lack of estimates as to the basic risk of the use of cyber weapons[[6]](#footnote-6). Digital interdependence between various sectors of the economy is likely to create situations where failure in one sector not only creates damage in another, but various mutually reinforcing feedbacks. It is thus clear that the cascade effect of any attack on systems and net structures in a closely interconnected world may be enormous, - and, as the assets of the attacker may also be endangered this may in the best case serve as an implicit deterrent[[7]](#footnote-7). Characteristically, all efforts to define cyber *weapons* have failed in the past, although some partial identification of dedicated attack malware has resulted.

The truth is thus that cyber attacks pose an even greater threat to society at large and its social and economic fabric than indicated in any variant of military doctrine, planning and forebodings. The growing dependence on digital technology puts public and private facilities, electricity supply, telecommunications, banking and finance, transportation, manufacturing, medical installations, education and government, just as much at risk as military assets (more on these critical infrastructures further down). We must speak of an *integral risk exposure* of our countries and their economies. In this perspective, the differences between cyberwar, cyber terrorism and cybercrime become blurred, and it appears more adequate to speak of cyber attacks and cyber conflict when analyzing the broad threat pattern now emerging and impinging so clearly on the economy. In popular parlance, cyberwar has often been understood with this broad connotation, as a reflection of the unspecified, but massive fear cyber conflict evokes among citizens. These public intuitions demonstrate that cybersecurity, or rather cyber insecurity, is among the great challenges of our time.

It is these broad threat patterns that most directly impinge upon the economy by way of an integrated threat perspective, and on which this essay will concentrate in keeping with the general theme of this book. A realistic economic risk analysis requires a comprehensive, integrated analysis of the entire spectrum of cyber risks, whether the primary purpose of a cyber attack is to reach economic gain or not, and an integrated strategy to combat cyber conflict. The vital contribution digital technologies make to our era and especially to economic security, depends on the functioning, integrity and reliability of these technologies, and of the confidence they inspire. Cybersecurity must thus be a central theme of this essay, as it was in the 2010 publication cited above.

We will, then, first explore the extent to which digital technology has already permeated all economically relevant segments of society. In a predictive mood, we will then analyze, even if somewhat speculatively, the likely growth and mutation of the digital world in years to come. The following chapter will focus on the vulnerabilities and exposure to risk this ever more interconnected world will generate, and the security threats thereto as they are shaping up. An attempt will then be made to measure the resulting economic damage, and the tenuous relationship between cyber attack and cyber defense, i.e. the state of the security industry. In the second part of the essay, the accent will be on counterstrategies, damage mitigation and prevention, exploring the full panoply of cyber defense. An important emphasis will be placed on the legal aspect, as there is as yet little provision made to effectively control the escalation of cyber conflict by norms, and as there is at best an incipient understanding of how the existing norms of international law would apply[[8]](#footnote-8).

**Cyber as the Agent of an Economic Paradigm Shift**

Any realistic threat assessment requires an overview over the state-of-the-art digital technology employed by key economic actors. Information and Communication Technologies (ICT) increasingly become the new dominant paradigm of all aspects of human endeavour, providing the all-encompassing operative system of human societies. Cyber Technology has become a defining characteristic of our age. The well-nigh total dependence on ICT confers vital importance upon the performance robustness, security and reliability of digital systems and networks, confidence in their functionality and integrity, and in the protection of privacy. These increasingly become framework conditions for the functioning of society. Information security thus needs to be ranked as an overarching societal challenge of global proportions.

The progress and growth of ICT which we currently observe in the economy and elsewhere, including in military affairs, is breathtaking and justifies designation as a *second digital revolution.*

As mentioned by different sources and studies, rapid advancements regarding the integration density and performance of very large scale digital circuits which form the base technology in the digital age will be going on for at least another decade. Moore´s law of doubling computer performance every 18 months continues to be valid. As these digital components are getting smaller and cheaper, more and more of these components like microprocessors, sensors and actuators are embedded in technical or physical systems and interconnected via various kinds of networks. According to a recent paper by Manfred Broy, currently about 98% of all microprocessors are embedded (and invisible), and are connected via sensors (e.g. RFIDs) and actuators with the physical world and with the internet. As Broy mentions “… the physical world merges with the virtual world of cyberspace leading to Cyber-Physical Systems and to an Internet of Things, data, and services”[[9]](#footnote-9).

With more than 2,3 bn computers on-line, billions of microprocessors and microcomputers thus employed in embedded systems, RFIDs and other sensors, mobile devices, evolving network technologies and bandwidth, ultra-miniaturization of digital circuits and the resulting ubiquity of new miniaturized computing elements, the steady progress towards an “Internet of Things” with miniature computers soon inserted in cloths or the frames of eyeglasses, the possible resulting threat spectrum goes infinitely beyond traditional computers and the current Internet. Basically, *all* digital devices and networks are vulnerable, and increasing interconnectivity of digital systems can easily result in “snowball”-like distribution of errors, faults and failures, - or damage caused by cyber attacks. And these are on-going processes. We are already witnessing an explosive growth of digital actors and an exponential growth curve of interconnectivities, an all-pervasiveness that automatically spells a parallel increase in vulnerabilities.

The phenomena of *migration* – migration of fixed line telephone to mobile systems and to VoIP, migration of computing processes, software management and data storage from individual and business computers to huge server farms (grid computing in the “cloud”) with petabyte capacity (1PB = 1015 bytes) and cloud computing services – and *convergence* – resulting in an undistinguishable mesh of mobile and fixed systems – add up to a huge integrated global network structure with a universe of connectivity.

Counting traditional computers, mobile devices, embedded systems – omnipresent, but sophisticated microprocessors often miniaturized to the size of a sugar cube -, some analysts estimate that the total number of interconnected systems, civilian and military, has already reached – or will soon be reaching – the level of 50 bn. The exponential propensity of their mutual connectivity potential – and thus also their vulnerability to cyber attack if not specifically protected – is difficult to calculate, but in any event a matter of evidence and concern.

The development of mobile devices is particularly noteworthy. Recent statistics indicate that worldwide smartphones trading alone will have reached more than 650 million units in 2012, bringing the worldwide mobile subscriber base to nearly 8,5 bn by 2016, an annual growth rate of more than 7%, with mobile penetration exceeding the point of 100% soon. The annual business figure of the mobile handset business stands at appr. US$250 bn[[10]](#footnote-10). This does not count in other mobile devices, nor the innovative potential of all smart mobile systems:such as smartphones, tablet computers etc. with mobile Internet connection. They are making computing ubiquitous.

In OECD countries and in emerging markets, nearly all companies are connected to the Internet, and an increasingly higher percentage of business sector value-added can be attributed to Internet-related activities; developing countries are catching up with increasing speed, often predominantly based on mobile techniques.

The production apparatus of our societies is already digitized to a large extent. Internet-connected machines that operate comprehensive autonomous machine-to-machine information exchange systems within factories, often interconnected through wireless protocols, so-called cyber-physical production systems, increasingly characterize today’s – and tomorrow’s – production processes and are the basis of the fourth industrial revolution, even though this development is as yet incipient. Net-connected and imbedded IT systems like RFID responders become the driver of innovation, replacing central production control and management by self-organization and fine-tuned process adjustments.

“Smart factories” go hand-in-hand with smart grids for essential public support functions. A rational energy economy has to move to smart grids, a production and consumption control and steering process predicated upon the functioning of millions of sensors. Smart systems are by no means the property of OECD countries: New Delhi has recently introduced smart grids for the energy management of the metropolis.

The *second digital revolution* manifests itself also in the unprecedented quantitative growth of data traffic. The new dimension of information storage, transfer and processing, and the availability of new ICT services is specifically enabled by the tremendous growth of data centers, “Big Data”, colloquially referred to as the “cloud”, which have become a prime driver of economic growth. The various and fast-growing “cloud” services (Infrastructure as a Service, IaaS, Software as a Service, SaaS, etc.) allow for the reduction of company hardware and software acquisition and maintenance, and offer flexibility, savings, and universal availability of company data from anywhere. The explosion of data production is indeed fomented by the cloud phenomenon. Cloud computing is the fastest growing segment of IT operations, with data in the cloud expected to grow six-fold over a five year span, and to produce, for the EU alone, almost 600 bn € additional revenue, creating 2,5 mn new jobs in the process.

**The Cyber World of Tomorrow**

Before appreciating fully the threats and economic risks of cyber conflict, one must also appreciate, if in a summary manner, *evolving* cyber developments, although predicting is risky business by itself. Yet, the grand lines can be drawn, as they develop from current trends, provided a realistic accelerator is built in. It is safe to assume that miniaturization and the all-pervasiveness of devices - the Internet of things, based on the much more potent Internet Protocol IPv6 - will continue at an even faster pace, that the ubiquity and pervasiveness of invisible computing will grow, that data growth will accelerate and that new forms of computing leading to different and novel structures of processing configurations in digital nets, e.g. neural computing, will evolve. We will see the development of minute computers with self-organizing potential (“organic computing”), able to communicate autonomously with other digital devices, new human mind-machine communications (to name just some of the “next generation” computing trends[[11]](#footnote-11)). These developments will generate a continuing explosive growth wave of digital devices, dwarfing the quantitative evolution we have seen so far. Computing power, especially through grid and cloud computing, becomes virtually unlimited. The incorporation of *smart* processing modes in industry will accelerate, and *smart grids*, today still in an experimental stage, will be a regular feature of the economic environment.

Broadband availability and coverage, and bandwidth, will increase to a point of providing entire societies, including in the developing world with effective and powerful on-line access, in many third world countries predominantly by mobile techniques[[12]](#footnote-12). We will see new very high speed fiber connections, and new high-speed wireless connections, two technologies that will shape the near future of connectivity. Mobile devices will become more sophisticated and versatile, - serving as means of payment, replacing traditional keys and even chip cards, able to receive high resolution television anywhere.

Mobile technologies will be so efficient that they allow work at home with full access to company data as a normal feature, thus changing the work structure and enabling savings in infrastructure and travel. *Bring your own device (BYOD)*, a work form where the employee takes on his computing and data management tasks from anywhere, fully connected, already in use in some companies today, will become a routine procedure. Nothing will be as before.

**Threat Development – the New Economic Reality of Cyber Insecurity**

The foregoing analysis has placed emphasis on the exponential current and future growth of systems and actors, all interconnected, that make up the cyber world. And it is evident that the multiplication of systems and actors are the principal indicators of new opportunities to imperil cyber security on a grand scale, military and in a civilian context. Growth of objects, at this exponential rate, indicates growths of threats, equally exponential. One must bear in mind that *any* digital object, if not protected, can be an object of cyber attack, and if it is part of a connectivity mesh, this spells multiple infection potentials and profusion of damage.

The tremendous growth process simultaneously affecting cyber systems, actors and net structures has generated the famous quantity to quality jump. Rather than old-style crime merely going on-line, cyber attackers are today taking advantage of the increasing dependence of our day-to-day life on IT by developing creative strategies to exploit the vulnerabilities of IT-systems.

The resulting change is nothing less but dramatic. The various dimensions of the threat surge have to be assessed in conjunction. The explosive growth of systems and interconnectivity, - here already described - , the growing intensity, sophistication and diversity of attack modes and attack technology, and the radical change in the characteristics of cyber conflict perpetrators, all interact and multiply the damage potential. With the *second digital revolution* we enter a new world of perils which makes analyses of the cyber threat of, say, ten years ago, appear idyllic.

All operations in cyber conflict have in common that they intervene in the functioning of digital processes, whether they affect data, their storage, their handling, or their transmission, thus undermining the reliability and authenticity, integrity and privacy of data and processes.

But the aim of an attack can differ. Some leave the normal functioning of the systems and computing processes unaffected: their purpose is to observe and possibly to copy (“steal”) data. The key applications are military and industrial espionage, data and personality theft. If the attack remains undiscovered for a length of time, it can be pursued, and even more data can be retrieved as they emerge; espionage and data theft operations aim at this long-term covert use. The usual term for these practices is *persistent threat*, or in case of an organized crime perpetrator and systematic use over time, *Advanced Persistent Threat (APT).*

Other attacks, using for instance “logic bombs”, aim at altering or destroying the functions of the attacked system, falsifying its effect (e.g. the operating instructions of a weapons system) or making it inoperative. Still other attacks change the normal functions for abusive or illegal purposes for a given time, for instances in bank or credit card fraud, or more permanently by defacing the sites. The massive sending of *spam,* unsolicited bulk e-mail, frequently with commercial content, to an indiscriminate set of recipients, can also be termed an attack, as it is frequently used to dispatch viruses and other malware as a technique to enact financial theft, [identity theft](http://en.wikipedia.org/wiki/Identity_theft), data and intellectual property theft, fraud or simply [deceptive marketing](http://en.wikipedia.org/wiki/False_advertising).

**Evolving Attack Modes**

The conflict modes which we will review subsequently, together with their development trends and evolving dimension, fall in one or several of these attack scenarios. As this essay does not purport to deal with their information-technological characteristics, the references to them will be general.

Topical information and figures are amply collected and made available by the globally operating cyber security companies Symantec, Norton, McAfee, Microsoft, KasperskyLabs, PandaLabs and CISCO, among others[[13]](#footnote-13). In addition, many national cyber security services like the German BSI, the US Homeland Security Department, and the European agency ENISA[[14]](#footnote-14) collect and often publish data. While extremely revealing, such compilations still have to be read with a grain of caution. Commercial IT security companies, while certainly correct and conscientious with their information, tend to highlight the perils of attack in the interest of their business. And victims tend to underreport incidents, - businesses, like banks, in order to protect business confidence, individuals because of shyness or lack of interlocutors, national security services, especially when information networks relate to military secrets, weapons systems, or an essential security dispositive that has been penetrated.

But it is exactly the exploitation of espionage possibilities that have been displaying lately one of the highest growth factors. As accessing the secure systems of target states, organizations and industries encounter increasingly lower barriers to entry, and the ubiquity of techniques used to undertake such collection, many of which have been developed by criminal groups, is evident, some States make an increasingly aggressive use of cyber espionage. There is detailed information on China’s cyber operations in the US, where the intruders concentrate on key corporate infrastructures aiming at the theft of intellectual property[[15]](#footnote-15). Since many years China has been practicing nuclear espionage, collecting highly classified information on long, documented lists of nuclear warheads, while also accessing networks of major defense and financial institutions. The most commonly used penetration technique is Trojan attacks, where a virus is introduced and can over long periods be instructed to download data without being perceived by the target system’s operator. While China’s cyber exploitation operations have received special publicity because of their extent and aggressiveness, all other great powers are also involved in intense espionage battles. At the moment, viruses with espionage functions enjoy a positive business cycle. Lately the spyware variants Madi and Flame have become particularly prominent[[16]](#footnote-16). Their appearance shows that even relatively simply constructed spyware can serve to obtain very valuable and sensitive information on a large scale.

From State-run espionage networks with a high Trojan penetration, it is only one step to the direct attack, degradation of weapons systems, and sabotage, e.g. through sleeping logic bombs, although these need to be able to resist the vigilance and on-going soft-ware upgrades of the soon-to-be attacked party.

All reports from security companies agree in their latest editions that malicious attacks continue to grow rapidly and, according to McAfee, have presently reached an all-time high in data-base breaches. At the same time there is growing sophistication of attacks and malware development. Mobile malware, a new central focus of attack, has almost doubled in a one-quarter period. With the number of vulnerabilities in the mobile space rising – Symantec has detected a 93% rise in one year - , and malware authors creating specific malware geared to mobile opportunities, 2011 was the first year that mobile malware presented a tangible threat to businesses and consumers, not least because workers tend to bring their smartphones and tablets into the corporate environment faster than many organizations are able to secure and manage them. “BYOD” poses enormous new security challenges. It may lead to a further long-term increase in data breaches. The new threats to mobile are designed for activities including data collection, the sending of content, and user tracking.

There are quantitative jumps in all categories of attack mode. Symantec alone blocked more than 5.5 billion malicious attacks in 2011, an increase of 81 percent over the previous year. In addition, the number of unique malware variants increased to 403 million during that period.

Financial damage to banks and individual customers (credit card fraud, phishing and carding, spearphishing, direct financial extortion) continues to rise fast. Last year cybercriminals set up an automated transfer system (ATS) that was used to attack European financial institutions, and set out to target a major U.S. multinational financial institution. “Mobile Money Transfer”, MMT, a catch word for novel digital financial systems, services that are bringing banking to millions of people in the Third World, will, if not quickly and effectively regulated, display the “dark side of cyber finance” and will become a playing field for cyber attack and crime[[17]](#footnote-17).

Given the still persisting quasi-monoculture of operating systems where one producer dominates the market, the vulnerabilities inherent in its products are particularly widespread and, if exploited, lead to substantial damages. The main source for distributing computer viruses are therefore innocent users of personal computers and company computers, who often are not aware of the risks inside the web.

Virus attacks have also been greatly facilitated by the huge presence of “new social networks” that act as gratuitous distributors for infection. Moving beyond spam attacks, cyber criminals are turning to these social networks. Their seemingly very innocent nature makes users incorrectly assume they are not at risk, and attackers are using these sites to target new victims. Due to social engineering techniques and the viral nature of social networks, it is much easier there for threats to spread from one person to the next. Yet spam, although now better controlled by anti-spam filters of the Internet Service Providers, and in addition in many countries subject to anti-spam legislation, is still rampant; more than 86% of Internet traffic – 62 bn messages globally per day - was spam in 2010, (with a slightly lower percentage of 75%, 42 bn messages, in 2011)[[18]](#footnote-18) which by inundating the accounts causes appreciable damage in lost production time, apart from its potential to spread virus attacks.

There is another move away from indiscriminate spam: attackers individualize their attack, focusing on those victims on whom they have previously accumulated actionable knowledge through data and personality theft. One individualizing method is [spearphishing](http://www.reuters.com/article/2011/04/04/us-hackers-epsilon-idUSTRE7336DZ20110404). The term denotes a targeted email attack on persons who are known to frequent specific online businesses and may have relevant account information for banks, specific businesses or distribution chains. It is so called because the move to target is precise and narrow, like the tip of a spear. Although credit card data may not be stolen, email addresses are compromised, and these addresses can be sold on the black market. Furthermore, the information gathered from spearphishing can also beget more sophisticated phishing attacks on other customers acting upon the legitimate looking message from a retailer or bank with whom they are already doing business. Targeted attacks are increasingly directed at smaller companies, because they may be less well defended or occupy an important place in a given supply chain.

At the same time, malicious code is less and less programmed to directly cause irreparable damage. Rather, attackers try to bring infected computers under their control so that they can continue to misuse them by way of Trojan infection and remote control.

One important and effective element in such schemes are targeted DDoS (*Distributed Denial of Service*) attacks. In this attack method, the attacker floods the server with useless data packages thus overloading the system in order to provoke business interruptions in the victim’s systems and net structures. In a business context, such attacks could be launched by competitors, dissatisfied personnel, or otherwise motivated groups of people. Obstructing the smooth operation of web sites massively can result in considerable economic consequences, especially for companies practicing or relying on e-commerce. In military or political conflict scenarios, DDoS attacks – a central feature of the cyber attack on Estonia in 2007, where, however, economic damage was minor - , can paralyze defense installations and communications, neutralize or destroy weapon systems, paralyze government services, provoke breakdowns in critical infrastructures and economic sectors, and may thereby, in extreme cases, lead to massive loss of life.

While the latest reports of the security companies clearly put their finger on the new threats to mobile devices – and through them to the whole interconnected universe – they do not yet quantify the new vulnerabilities that spring from the explosive growth of the cloud centers. Yet, apart from the mobile threat, the insecurity of massive migration of data to the cloud has for some time been a hot topic in security discussions as, in the words of an ENISA report from 2009[[19]](#footnote-19), “The massive concentrations of resources and data present a more attractive target to attackers”, although the agency believes that “cloud-based defences can be more robust, scalable and cost-effective”.

Underpinning this list of new attack modes is the emergence of a wide array of new highly sophisticated destructive software programs appearing with an ever increasing rapidity and sophistication[[20]](#footnote-20) and targeting precision. National boundaries are of course no longer relevant to this type of threats, and it is impossible to confine the protection of information technology and IT infrastructure to domestic policies. The authors and vendors – and profiteers - of computer viruses and other malware are operating globally, and cyber defense has to adopt that same mode.

**The New Enemy: Collective Actors of Cyber Conflict**

Internet criminality is more and more conducted in a professional and commercial manner. Targeted attacks are increasingly carried out by organised criminals. Financial interests are the decisive driving power. Cyber conflict is developing into a powerful branch of the international organized crime scene. Crime consortia command armies of cyber experts and malware developers and systematically organize crime campaigns for gain. Over years of operation they have built professional teams for sophisticated malware development, benefitting from massive crime-generated resources. This also allows for a new magnitude of attacks. Already in 2004, sixteen percent of hacking activities were aimed at e-commerce companies. This represented a 400-percent-increase compared to the previous year, but since then the individual hacker has terminally faded into the dark, and organizations have taken over.

They systematically plant Trojans into large numbers of computers – increasingly also into mobile devices, and thus have thousands and even millions of devices at their command where they can activate malware and use it for attacks, *Botnets* – the word is composed of robot and net - are on the rise. These aggregates of *zombie computers*  have several uses. Their operators – the *botherders* - can proceed to money-making directly, or collect espionage knowledge, commit data and identity theft. Botnets provide an effective and increasingly used infrastructure to distribute spying programs in a wide range of variants, and to do business in online-banking. Botnets are the ideal platform for DDoS attacks, as these need a large number of activated email-emitters to reach the desired large-scale saturation effect. Botnets can also be rented out to other criminal perpetrators, - or to Governments, as digital mercenaries, creating an opaque State-non-State actor mix.They are not the only merchandise on the black market, accessible to criminals and governments alike; aggressive attack software, email addresses and credit card numbers in huge packages are available for almost token prices. There is no lack of *zombies* either. Almost every 10th e‑mail is estimated to be infected by relevant viruses, and, accordingly, the botherders can count on large herds, functioning unbeknownst to their owners. Already in 2010 McAfee had estimated that the number of *zombie* computer grows by at least 5 million systems per month, and that identified malware variants increase annually by a factor of 5. At the best time of the *Conficker* virus which was, and is, autonomously able to recruit new computers into the botnet, the dimension of that net alone may have reached more than 10 mn devices. Without the push of the new collective actors this growth would be inconceivable.

One alarming aspect of the new criminal cyber scene is the aforementioned technical and financial prowess to develop malware *ahead* of cyber defense and in spite of the undoubted efficiency of the international cyber security industry. At the same time, the digital dependency of modern societies is growing; infrastructures are ever more net-dependent (e.g. smart grids). Even the numerical aspect alone is worrying. McAfee’s reports indicate that identified malware variants increase annually by a factor of 5. The timeless dilemma of attack vs. defense thus takes on a new meaning, especially due to these new collective operators in cyber space, and the defenders of a functioning, peaceful and crime-free cyber space do not always have the upper hand[[21]](#footnote-21). The attack potential of these organized evil forces also gives an idea of the possibilities of a true cyber war if states and organized crime cooperate.

There are several analyses with theories about the countries or places of residence of these crime groups, based in part on the URL of the attack messages. But given the unlimited possibilities of station-hopping and combining inputs from various sender countries, this essay refrains from any such attribution.

With all these developments it has certainly become clear, that the term *security* has reached an entirely new meaning and dimension in cyber space; national boundaries provide less protection today than ever before. Such terms as internal and external security are increasingly difficult to define or might indeed merge in most cases.

Cyberterrorism can also be subsumed under the new collective threats. Under the dominant definition, cyber terrorism denotes the use of Internet attacks by political-ideological groups, aiming at large-scale disruption of systems and networks, potentially creating destruction, alarm and panic. If the purposes of these terrorists are not economic gain, they would not be genuinely within the purview of this study. If they go economic, for instance, to extort funds for the financing of terrorist activities, they are not essentially different from other criminal operators, and would only form part of the integral cyber conflict and threat landscape here described. That does by no means trivialize the dangers they pose, especially with attacks on critical infrastructures, and they are rightfully within the focus of governments in their anti-terrorism and general security campaigns[[22]](#footnote-22).

**Measuring the Cost of Cyber Conflict: Is Quantifying Possible?**

Several international cybersecurity companies periodically undertake to put a price tag on overall economic damage caused by cyber conflict, based on their own activities and insight.

The Norton Cybercrime Report 2012 calculates the immediate financial loss to come to US$110 bn for 24 countries (Symantec arrives at 114 bn), with 556 mn victims; but if the money equivalent of lost time trying to respond to incidents and resolve cybercrime is added, the figure rises to roughly 390 bn. Whatever the exact methodology in arriving at these figures, it is certain that – apart from the limited number of countries covered – the cost of long-term damage and business disruption, direct cash spent in incident response, and the damage to business reputation have not been fully factored in, and, for all countries, if included, should reach important additional proportions. And as pointed out before, any damage statistics have to cope with the huge number of unreported and unassessed attack cases[[23]](#footnote-23).

Preventive and cyber defense measures do not appear to be covered either. Taking the US Government efforts at enhancing its cybersecurity capabilities (protecting critical infrastructures, cybersecurity operations, information sharing and analysis, etc.) as an example, the budget allotment of the Department for Homeland Security for these purposes alone amounts to US$1,2 bn for FY 2013[[24]](#footnote-24), surely less than the private sector, all businesses told, has to invest in cybersecurity and cyber vigilance. Such amounts of funds have to be scaled up for the entire international community. The cybersecurity industry itself runs a multi-billion euro or dollar business.

Estimating the budgets for safeguarding military installations, communication systems and weapons will be even more difficult. But it is evident that the availability and maintenance of one’s own military communications and command structures as well as the capacity to neutralize hostile military action – cyber defense – must enter, as they do, into calculation and planning.

Given the uncertainties of calculation, it is thus not surprising that there are no handy overall figures. Yet, at the recent First World Summit on Cybersecurity organized by the EastWest Institute in Dallas, Texas, in 2010, authoritative speakers have estimated the total economic damage of cyberinsecurity at appr. US$ 1 tn (1000 billions) annually, and this indicative figure has been used since without anybody seriously objecting. In the same order of magnitude, an authoritative speaker from the US House of Representatives has estimated the annual loss from cyber espionage – presumably from Chinese intruders – to have reached $300 bn in 2012, - no breakdown of figures included[[25]](#footnote-25). At the World Economic Forum at Davos 2013 it has been assumed that over the next decade there is a 10% chance of a major digital breakdown – presumably of criminal origin - costing over a quarter of a tn dollars[[26]](#footnote-26). These figures, and at least their order of magnitude, are enormous.

**II.**

While the *first part* analyzed current and evolving cyber threats and their enormous economic cost, and emphasized that an integral risk situation required also a comprehensive and integral response, this *second part*will concentrate on combating cyber conflict, developing cyber defense strategies and devising strategies for the mitigation of consequences.

**Limits on Cyberwarfare Proper**

Although we have found the concept of cyberwar to be ambiguous and of doubtful relevance to the present analysis of economic risks, a brief summary of the constraints international law places on hostile cyber action appears in order, as they may limit the potential of damage.

International law and especially the law of armed conflict antedate the cyber age, but as cyber space is now increasingly recognized as a new theater of war, it is generally assumed that the *jus ad bellum*  and the *jus in bello*, suitably adapted, also govern hostilities in cyberspace. There is much academic literature on the analogies that can and must be drawn from the UN Charter, the Hague, Geneva and ICRC Conventions and Additional Protocols and other treaties on Humanitarian Law, UN General Assembly resolutions announcing general principles for state conduct, extant international case law and customary International Law. Governments have published manuals and cyber strategies that also define constraints, but at the same time provide the underpinning for huge investments in cyber armament. Much of the debate centers on the definition of “attack” and “armed attack”, but also cyber-suited definitions on the principles of the laws of armed conflict (necessity, distinction, proportionality, non-discrimination, prohibition of attack on civilian objects and certain persons, objects and activities, neutrality etc.[[27]](#footnote-27)

The views expressed range from the acceptance of broad options of attack, where targeting critical infrastructures is considered within the realm of legality[[28]](#footnote-28) to more restrictive interpretations[[29]](#footnote-29).

There is no point in belaboring these various perspectives, as the principal reference work is now quite clearly the recently published “Tallinn Manual on the International Law Applicable to Cyber Warfare”[[30]](#footnote-30) elaborated by “The International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence”. This comprehensive treatise seeks to establish 95 “Rules” covering the *jus ad bellum* and *jus in bello* for cyber conflict exhaustively.

The Manual has obvious merit. The prestigious assembly of co-authors proposes under the international regime *de lege lata,* plausible definitions and rules and puts an end to many previous controversies. Yet, the members in dealing with the military-civilian relationship, and in trying to distinguish between military and civilian assets, and dealing with non-discrimination, etc. have to admit that cyber “weapons” “by their nature generate effects that are incapable of being controlled and therefore can spread uncontrollably into civilian and other protected computers and computer networks that create an uncontrollable chain of events” (p.122), and that most possible targets, especially critical infrastructures and cyber infrastructures, are dual-use, and that an attack on them creates more than the “collateral damage” to be assumed in kinetic conflict. Could a critical infrastructure of mixed military-civilian use also be targeted if it supports targets that are protected by the Geneva Conventions? The Manual seems to give preference to the military purposes. Rules such as “The civilian population as such, as well as individual civilians, shall not be the object of cyber attack” (Rule 32) thus are likely to lose their protective effect. Rules 14 and 55, specifying that cyber operations in self-defense must be necessary and “proportionate” become blurred, if, because of lack of controllability, the proportion cannot be measured reliably. Other uncertainties concern the treatment of hidden non-State actors, combatant status, definition of “war-sustaining” economic objects, neutrality, anticipatory self-defense – when can a cyber attack that occurs with lightning speed be judged to be imminent? The authors are more successful in defining “attack” and “armed attack”, employing the “effects” rule in the latter (“Whether a cyber operation constitutes an armed attack depends on its scale and effects”, Rule 13)[[31]](#footnote-31). Yet, even here the ambiguities are preoccupying. The “armed attack” rule is so broad, that it lowers the barrier to war; it is unwise and dangerous for international stability to treat conflicts that imply no clear threats to human lives or essential societal disruption as “armed attack” with the accompanying consequences under international law[[32]](#footnote-32).

On the whole, the Manual, far from constraining the cyberwarfare option, rather underlines the great new possibilities of cyber attacks and the uncontrolled damage it can inflict. Very little harnessing is done. Instead, the uncertainties and the risk to civilian cyber structures become more apparent. That refers specifically to Critical National Infrastructures which are not only predominantly privately owned, i.e. part of the national economies, but indirectly penetrate the whole social fabric so much that economies are ever more dependent on them. Cyber attacks on them not only generate massive economic damage, but also seriously compromise the security and safety of society, putting human life at peril.

More importantly, the Manual accepts the option of warfare in cyberspace in an unreflecting way and dodges the question whether unbridled cyber armament in view of future use is a wise course for civilized nations to take. The Manual starts of course from the underlying assumption that state-sponsored cyber hostilities respect the UN Charter, and are only invoked in self-defense. Yet, the final impression is that the whole-sale transfer of the traditional Law of Armed Conflict and the thinking in military terms does end up as a cloak of legitimacy for the cyberwars of the future, neglecting the huge dynamics both of digital developments, and the growing societal vulnerabilities and unpredictability of consequences.

A similar approach can also be detected in the military cyber manuals many governments have prepared, to the extent that they are publicly accessible.

Some countries are incorporating offensive cyber capabilities into conventional warfare strategy, foreseeing conventional military responses even to information *sabotage on the Internet, even independent of the presence of an “armed* attack” or human casualties. Others call for unlimited use of cyber weapons („exploit potential fully“, „maximum effect“, „joint firing process“, „retaliation“, „punishing blow“) indicating that planning also follows military lines („war-fighting doctrine“) with the corresponding analogies and thinking patterns[[33]](#footnote-33). Yet, concepts like deterrence, retaliation, „rules of engagement“ do not take account of the specificity of cyber attacks and, for instance, the problems of attribution and proportionality.

Fortunately, these concepts do not stand uncontradicted. The destruction potential and unpredictability of cyber attack options are increasingly recognized, and have nuanced the purely military viewpoint or are juxtaposed to it. In many military and political doctrine documents cyberwar prevention, prioritarisation of cyber defense, and cooperation of all stakeholders are now moving to the foreground. One interesting example is the US Department of Defense Strategy of Operating in Cyberwar of July 2011 which clearly opts for cyber defense, close cooperation between Government agencies, Government and industry and international cooperation. NATO’s summit documents, like the Declaration of Lisbon (20 November 2010) do not conceal defense needs, place the emphasis however, on central cyber protection and the optimization of collective cyber self-defense and internal alliance cooperation as well as international cooperation (§ 40). It is also significant that cyber attacks are not subsumed under the attack concept of Art. 5 of the NATO Treaty, but rather mentioned in the context of the consultation regime under Art. 4.[[34]](#footnote-34)

This indicates that the mastering of cyber attacks is in many quarters healthily recognized as falling under a new security paradigm that places prevention, „resilience“, strengthening of threatened digital infrastructures and a defense „network of partnerships“ up front.

As this article will substantiate further down, this movement to a defensive mode should lead one to introduce the concept of *cyber peace*.

To opt for the positive side in the war-peace antinomy implies an important change in perspective and scale of priorities, as it orients the mind towards the benefits and positive potential of the Information Society and provides a goal post to that effect, reinforcing the negative connotation of cyberwar and related terms and calamities – delegitimizing it as it were -, and fomenting dynamic movement towards a global culture of cyber security.

In attempting to reverse the above described belligerent perspectives one must be fully aware that digital infrastructures are now all-pervasive, and will unavoidably also be used for hostile, non-peaceful purposes. The over-riding objective, then, is to harness such uses and to provide the strictest possible limits for any attack situation. As the very term “cyberwar” is conducive to stimulating thinking in military categories, an attempt must be made to combat this mental automatism and to substantiate a plea for peaceful behaviour in cyber space.

**Active and Passive Cyber Defense**

If an “armed attack” is carried out by a State – or if such attack is presumed – the victim, the attacked state, has, under the UN Charter, the right to proportionate self-defense. But if the attack inflicts damage on private interests, e.g. an enterprise or a privately owned infrastructure (energy, banking, aviation, etc. – for a more precise definition see fn. 42)? Can the attacked then slap back? And can he do so also if there is uncertainty as to attribution and the perpetrator is, or may be, a non-state actor or simply an ordinary cyber criminal? Here national cyber law with its penal sanctions and law enforcement tools comes into play. The debate as to whether “active” defense is legal, even though it implies intrusion into systems and networks and inflicts damage, has been waged for some time[[35]](#footnote-35).

Active defense tactics such as have been proposed could include hacking back into systems to retrieve data, shutting down systems, sabotaging data, infecting the attacker with malware, taking over the attacker’s botnet, or hiring a botnet to attack the attacker. Feeding an attacker data (so long as it is not malware) may not be illegal, but these other active defense actions likely are. Just because actions are being taken against a criminal attack does not make them legal in most jurisdictions. Moreover, these actions can trigger lots of other laws (particularly if botnets are involved), such as intellectual property, spam, fraud, contract and tort laws. Plus, they can cause collateral damage to third party systems[[36]](#footnote-36).

Some of the justifications that are being suggested for active defense tactics include self defense, hot pursuit, and ownership of stolen data. However, none of these justifications hold water; self-justice will not do, and the right course to take instead is to make systems and nets more resilient, and to improve (passive) cyber defenses and national and international law enforcement[[37]](#footnote-37).

**An Emerging Comprehensive Information Security Management System**

After the foregoing excursion into the territory of cyber warfare with its ambiguities, deficits and scary implications, the discussion shall now once again focus on the overall threat panorama, with cyber conflict originating from states, non-state actors – or a combination of both - , terrorist groups, organized crime consortia, and cyber criminals in general. Commensurate with the near total penetration of our societies by cyber technologies, one can now increasingly observe that international organizations, governments, the economy in general, the IT industry and IT security industry, as well as civil society, - the entire *stakeholder* *community* as the accepted term goes, join forces to combat and mitigate threats in cyberspace. In a paper of limited length, this movement, in part concerted, in part autonomous, is impossible to cover. Thus, an attempt will only be made to list and evaluate its major forms of expression. The overriding key words are cyber defense, self-protection and resilience.

Resilience – the defensively oriented policy that maximizes the ability of possible target systems to prevent, deter and withstand cyber attacks and, if they occur to minimize and mitigate their effects – is a multidimensional concept and has technical, organizational, political and legal components that need to be combined to be effective[[38]](#footnote-38). We will discuss in turn the legal framework requirements, the requirements of self-defense at enterprise and end-user level, the improvement of attack-resistant technical design, the potential of standard-setting and best practices, the benefit of redundancies and societal assistance and cooperation, international cooperation and law enforcement, the role of information exchange, warning systems and emergency responses, and, of crucial importance, the national and transfrontier protection of Critical Information Infrastructures.

**Creating a harmonized legal framework to combat cyber crime and cyber conflict**

Cyberspace could not remain a lawless space, and with the advent of ICT legislators have faced a double task: capturing the new technologies within their national legal system, and to provide a harmonized international framework for penal prescriptions and sanctions and law enforcement, as cyber attacks can take their origins in any part of the globe. Most industrialized countries have now cyber laws and cybercrime laws, many of them very adequate, but significant variances in defining what constitutes a cyber offense, in detecting and identifying cyber crime, and in the applicable procedural provisions have until recently significantly hindered cybercriminal investigation. The Council of Europe Convention of Cybercrime[[39]](#footnote-39) (Budapest Convention, signed in 2001 and entered into force in 2004) has brought a major advance in the harmonization of global cybercrime laws, and I join Professor González Cussac in his praise of this instrument; I also agree with him that new digital developments and attack mode will make a revision of the text necessary over time, however valuable it is at this moment[[40]](#footnote-40). Yet, the Convention, as of this writing, has only been signed and ratified by 39 countries, with 10 ratifications pending. Significantly absent are Russia, China, as so often Israel, and most third world countries, presumably reticent to adopt a document of European origin. The ITU Toolkit for Cybercrime Legislation has been developed as an alternative, with proposed legislative language that is harmonized with the Convention and cybercrime laws in industrialized nations. Broader use of these texts, or adopting comparable autonomous language by countries not yet party to the Convention will hopefully soon advance the harmonization process further. This is time-critical. The Convention, of course, has to be translated into national legislation by countries ratifying the international legal commitments..

**Self-Protection**

Cyber defense begins at home or at enterprise level. Among the obvious obligations of the Chief Information Officer should be the introduction of state-of-the art firewall, antivirus and incident information technology, encryption of confidential information, access control for premises and digital equipment, including a rigorous and differentiated password management (“need to know”) and other sophisticated authentication techniques. If BYOD is permitted, rigorous controls should cover the brought-in equipment. Vigilance is especially required as regards the SCADA systems of critical infrastructure installations, as these are particularly vulnerable to state, non-state or terrorist attacks with a military or otherwise disruptive purpose. This should be obvious, but experience demonstrates that theft of confidential information, both in enterprises and governmental agencies, is predominantly due to negligent insiders. More than 9 out of 10 breaches would have been prevented if the organizations had followed data protection and information security best practices[[41]](#footnote-41).

One of three top causes of data breach is physical theft or loss of devices. Also, a report from German industry shows that only a small percentage of e-mails with highly sensitive information, like industrial design blueprints, are encrypted. There is a systematic lack of encryption on mobile company devices. In many cases, no provision is made for redundancies that could, in case of attack, conserve or rapidly re-establish functionality of systems or connections. .

**Designing for Security**

One important loophole for attackers almost from the inception has been that hardware and software designers, focusing primarily on design benefits arising from technical advances for performance, have given less interest and effort to information security and privacy. Also, building in security from the outset may entail additional cost reducing profit margins. Traditionally, there has been a gap between the production and the security industries, helped by the lack of awareness of end-users of information security and privacy risks inherent in their equipment; for a long time, there has been incongruence between factual and perceived security. Many smaller enterprises may not have the resources or profession skills set to design the means of protection themselves. These gaps are now increasingly filled by a more security-conscious industry, higher end-user awareness, closer cooperation and even common ventures of the various stakeholders (see, for instance the recent acquisition of the important IT Security company McAfee by Intel).

Also it would be wrong not to give credit to major industry alliances formed to promote the security performance of hardware, software and net architecture, collective exercises that have started mostly in the nineties of the last century. Most prominent is the Trusted Computing Group with more than 100 members, contributors or adopters from industry. Its Trusted Platform Module (TPM) has been standardized by ISO/IEC[[42]](#footnote-42).

Yet, given the threat landscape, the obligation of the hardware and software industry to “design for security” remains permanent, and there is also a permanent responsibility for public and private institutions and for countries to establish security procurement and certification policies and standards[[43]](#footnote-43). Collective efforts to securize SCADA system design would appear particularly useful. All this is based on the insight that there is still a lack of design and analysis methods, scientifically proven, to master the enormous complexities of future interconnected digital systems, especially regarding safety, reliability, functioning and security. The IT security industry deserves high marks for keeping abreast, at a very professional level, of the challenges it increasingly has to confront; the security companies run a rapidly expanding and highly demanding and competitive multi-billion dollar business.

**Standard-Setting and Best Practices.**

Government action and self-organization by industry have created a universe of technical and operational standards to secure IT structures. Many of these are voluntary, but a system of certifications provides incentives to adopt them with public visibility. Enterprises that do not vie for excellence in this area, and consequently suffer attacks and data breaches, not only lose money, but also reputation and clients. The most important standards for the management of IT technology, of practically global applicability, have been elaborated by ISO/IEL[[44]](#footnote-44) in the series 27.000 and 13.335, for the aforementioned Trusted Platform Module in norms 11889-1 to 11889-4 on information technology (2009). In the USA the norm-setting function is entrusted to the American National Standards Institute ANSI. For years, the community of users, developers and vendors of Internet technology have joined in the Internet Engineering Task Force (associated with the Internet Society) to develop and promote standards for the Internet infrastructure, routing, transport security. Then, on the special problems of distributed computing, there is the Open Grid Forum for standard-setting in grid computing and grid architecture.

The International Information Systems Security Certification Consortium (ISC), described as “the world’s largest IT security organization” (“security transcends technology”), promotes the standardization idea by awarding certificates for excellence in secure IT operations (Certified Information Security Professional, CISSP); the areas eligible for certificates also include software development, security architecture and design. 85.285 members from 143 countries currently hold the certificate. The issuers of certificates beyond the traditional norm-setting agencies, - institutes, associations, individual enterprises, intergovernmental agencies - , are many, obviously reflecting a need for recognition of excellence and confidence-building. An indicative compilation on the Wikipedia webpage of CISSP lists 70 different certifications[[45]](#footnote-45).

**Protection of Critical Infrastructures**

CIIP, the protection of critical information infrastructures[[46]](#footnote-46), has for many years been at the center of attention of information security policies and strategies to enhance resilience, both on the part of Governments and international bodies, and of the operators of these infrastructures themselves. Indeed, in a “cyberwar” context , it would be the center piece of defensive strategies and of any effort to optimize system resilience. Given their vital importance for the functioning of society, the increasing vulnerability of infrastructures in an interconnected and Internet-dependent environment, and the possible cascade effects of their failure, this priority is understandable. Critical infrastructures are in the first in the line of fire of military attack, terrorists, and crime consortia – organized crime –, in the latter case as a basis for blackmail.

In the US, presidential directives since the time of President Clinton have ordered the necessary protective measures. Securing critical infrastructures and information systems is an essential part of the brief of the Department of Homeland Security, generously endowed in each annual budget. CIIP policies figure prominently on the DHS home page www.dhs.gov. Capping intense previous efforts, the US President on February 13, 2013 signed an [*Executive Order (EO) on Improving Critical* I*nfrastructure Cybersecurity*](http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) and *a* [*Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience*](http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil) which provide instructive reading. Another major actor is the European Commission, assisted by its net security agency ENISA. Mindful of the still existing differences in systems and levels of protection in the 27 member countries, the EU has been working on CIIP and the harmonization of protection standards for some time. In 2009, the Commission adopted an Action Plan and a Communication on CIIP[[47]](#footnote-47) and has organized a EU Ministerial Conference on CIIP[[48]](#footnote-48). The European Public- Private Partnership for Resilience has already been referred to. ENISA has been organizing several European Cybersecurity Exercises with broad government and private sector participation, the latest in 2012[[49]](#footnote-49), aiming at strengthening the cyber incident management community. On February 7, 2013, the Commission published, in a Joint Communication with the other major EU bodies, the Cyber Strategy of the European Union which, in a broad sweep intends to set common minimum requirements at the national level for each member of Network and Information Systems (NIS), touching very much on resilience and infrastructure protection[[50]](#footnote-50). The European Parliament is also active; it held its latest meeting on CIIP on February 6, 2013.

For more than a decade the International Telecommunication Union (ITU) has been dealing with Critical Infrastructures Protection in a global perspective, lately in reference to its Global Cybersecurity Agenda, although no uniform regulatory framework has as yet emerged. Yet there is a wealth of studies, publications and conference reports, easily to be found at the ITU web page and that of its executive arm, the International Multilateral Partnership AgainstCyber Threats (IMPACT)[[51]](#footnote-51). The foregoing survey is no more than indicative; supplementing it with an overview over national initiatives would exceed the possibilities here. Yet many, if not most countries participating in the cyber world, deal with CIIP in their national organs, complementing international efforts. The German Federal Information Security Agency, for instance, runs a specialized Internet Platform for CIIP and sponsors a series of publications[[52]](#footnote-52).

**Resilience in Cloud Computing and Mobile Computing**

The rapid advance of cloud computing in huge data centers, and the massive migration to mobile as described in earlier sections of this article make it useful to analyze the resistance to attack of both these new venues of data management and cyber operations, and to point to novelties in this respect.

Cloud computing is a new way of delivering computing resources, not a new technology. The concentration of data and services delivery, scalable to demand, offers huge economic benefits and accordingly has attracted massive global investment. The worldwide forecast for cloud services in 2013 indicates a likely volume of $44.2 bn. As ENISA has tangibly expressed it, the cloud’s economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defenses can be more robust, scalable and cost-effective. Attacks on data centers of this dimension offer a military or terrorist attack important new opportunities, including tampering with the energy supply entailing massive loss of data (if energy supply redundancies are overcome), physical destruction, or cyber intrusion into the data bases. Clients’ fears are heightened as data masses are moving seemingly arbitrarily and untraceably from rack to rack, as supervisory personnel becomes anonymous, and as confidence in the integrity and privacy of the data becomes harder to maintain. The risks in cloud computing are major, and provide a major security challenge.

It is thus not surprising that cloud security has become a central theme of the current cybersecurity debate. In the very competitive cloud market, suppliers and security companies outdo one another in confidence-building. They can indeed show that there is also a premium in cloud security management. All kinds of security measures are cheaper when implemented on a larger scale; the same amount of investment in security buys better protection (cheaper physical perimeterisation and access control, better scaling of resources, timeliness of response, more effective threat management, etc.) Clients – governments among them – make their economic choices in good measure on the resilience of security services offered, reputation of confidentiality, and transparency of the internal center procedures. Lately, one important differentiating factor has been for European enterprises that they judge the legal data protection in Europe better than in the US, given the more intrusive data policy of the Department for Homeland Security.

Cloud security currently appears to be everybody’s business. The references of this article to current analytical work and recommendations on the subject are therefore limited to ENISA’s recent studies, “Cloud Computing: benefits, risks and recommendations for information security” – mentioned before - , and “Critical Cloud Computing: A CIIP perspective on cloud computing” (14 February 2013), both at [www.enisa.europa.eu](http://www.enisa.europa.eu).

Further up, figures have been cited on the breath-taking growth of the number of mobile digital devices, mobile services and applications, and the consequences of the migration to mobile technologies. It had also been pointed out that the threat to mobilecomputing and communication is growing out of proportion, making cyber attacks to mobile one of the dominant features of the threat landscape. Although exceedingly vulnerable to cyber attacks, mobile systems have long gone virtually unprotected. Only at this juncture, new anti-attack software for most mobile operative systems appears on the market. But the future may well lye not in software downloads to individual devices, but in central vigilance of mobile customers from the cloud, such as an alliance between Vodafone and BAE Systems is presently introducing into the market via a 5 year strategic partnership[[53]](#footnote-53). The promise of this cloud vigilance approach is that not only smartphones, but also tablets, and eventually smart RFIDs, the controlling systems in smart factories and other cyber-physical systems could be effectively protected.

**National and International Cooperation in Cybersecurity**

Given the seamless and global nature of the digital net structures, broad

national and international cooperation of the entire stakeholder community in combating and mitigating the consequences of cyber conflict is a matter of indubitable necessity, - and this necessity is globally recognized. The cooperation patterns that in part already exist, and need to be enhanced, include effective information exchanges including incident reporting, mutual assistance, also to activate redundancies, organized incident responses, warning systems, contact points within and between nations, improved cooperation on law enforcement, - and the organizational prerequisites to make all these desiderata function.

These measures –and other, related ones - appear quite straightforward and their usefulness within a strategy of preventing, defending against, sanctioning and mitigating incidents of cyber conflict is fairly self-evident. It is thus not surprising that the categories and numbers of stakeholders involved in them are huge and multifarious. We are dealing here with on-going and expanding processes, very hard to capture in a brief analysis. Suffice it to mention a few recent developments to indicate tendencies.

Entrusted by the World Summit on the Information Society with coordinating cyber security responses, the ITU has worked out a Global Cybersecurity Agenda that promotes many of the cooperation tasks globally, culminating in “ a framework of a global multi-stakeholder strategy for international cooperation, dialogue and cooperation”. The Agenda has dynamically pursued its goals, as can be gathered from the ITU web pages.

One important element of cooperation strategy is time-critical information across borders. The key mechanisms is the “24/7” approach, the permanent availability of contact points for cyber incident management. The first international plan originated with the G8 in 1998. The group created a 24 hours network of law enforcement experts among its members, but other governments joined. In the EU, the first 24/7 program came with the Council Framework Decision on attacks against information systems of 2003. A more systematic approach is part of the (Budapest) Convention on Cyber Crime which, apart from harmonizing criminal substantive law of cybercrime, has provided for domestic criminal procedural law powers necessary to investigate and prosecute such offenses, but has also set up a fast and effective regime of international cooperation and mutual assistance (art. 23 et.seq. of the Convention) for “trackind and tracing” that includes rules on the expedited preservation of stored computer and traffic data, etc. In art. 35 a permanent 24/7 network with appropriate equipment and trained personnel is set up in order to ensure the availability of immediate assistance for purposes of investigation and prosecution, including the collection of evidence and the locating of suspects. Many governments, even beyond existing treaty obligations, participate in the 24/7 set-up.

An element of growing importance in the incident reporting, mutual assistance, early warning , risk information etc. area are the Computer Emergency Response Teams (CERT), also labelled Computer Security Incident Response Teams (CSIRT). Pioneered by Carnegie Mellon University with funding from the US Department of Defense in 1988, the CERT is now a network of global dimension. In many countries there is a central government CERT, mostly charged with the coordination of other national CERTs and specifically with securing government digital infrastructures.

CERTs are teams of IT experts that follow and process information on computer incidents , analyze, advise, coordinate, lend assistance in combatting cyber attacks and in restitution, and often issue news bulletins and warnings on new threats. World-wide there are presently more than 250 organizations that use this name and deal with cybersecurity responses. In many countries industry and academic institutes have taken the initiative to establish CERTs. In the US, the Department of Homeland Security has established the US CERT. It coordinates CERT/CC, the in part federally funded US CERT community led by Carnegie Mellon. In Germany, a similar taks is fulfilled by the BSI with its CERT-Bund, in Spain with the Centro de Respuesta a Incidentes de Seguridad TIC by INTECO, an organ of the Ministry of Industry and its executive office red.es. The ITU, as part of its Global Cybersecurity Agenda, assists developing countries in creating national CERTs. In Sept. 2012, the EU has set up a CERT-EU, at first for the protection of its own entities, but also to liaise with national and government CERTs in the EU area. At the same time, in its Digital Agenda for Europe of 2010 the EU has called on members to establish their own national CERTs, a development to be completed by 2012, thus paving the way for an EU-wide network of effective incident responses.

In a related move, the EU has, in February of 2013, created a European Cyber Crime Centre (EC3) at EUROPOL that is to focus specifically on organized groups aiming at large criminal profits, and their hostile impact on infrastructures with enhanced investigative powers.

In the future it is necessary that the CERT movement be universalized, and that CERTs become more operative and interconnected, but they certainly form a major defensive weapon against cyber attack and to harness cyber conflict[[54]](#footnote-54).

At the time of this writing, one does not only observe a surge of cyber attacks on governments and industry, mostly in the APT vein, but alsoa growing awareness that all stakeholders must become more active and forthcoming in information exchange and sharing of cyber defense resources. One prominent example of such broad industry self-help endeavors is the collective cybersecurity alliance pioneered in Europe by René Obermann, the CEO of Deutsche Telekom, who has called for more voluntary incident reporting and transparency[[55]](#footnote-55)

**A Culture of Cybersecurity: Norms of Behavior for the Cyber Age**

So far, only *some* broad legal aspects have been dwelt upon: International Law as it ambiguously defines the limits to cyber warfare and “armed attack”, and the harmonization of criminal cyber law in its national and crossfrontier dimension. Not mentioned, but valid in most countries is, of course, a civil law regime that governs torts and damages, as well as the pertinent International Private Law.

But all that is far from filling the requirements of a functioning cyberspace regime able to combat and withstand cyber conflict. Legally speaking, the new area of cyberspace was initially a void, in need of a comprehensive framework of norms not only for states, but for all stakeholders. The task was to develop over time a set of norms for convivial behavior – of a culture of cyberspace and cybersecurity, including a comprehensive legal framework to manage and control the all-pervasive, infinite potential of digital technologies. Consequently, there is as yet little or no ability to effectively control by law the escalation of cyber conflict and to guarantee the peaceful use of cyberspace, - and as we have seen no unambiguous understanding of how the existing norms of international law would apply. A dangerous, precarious state of affairs indeed. The cybersecurity group within which I have been active, the World Federation of Scientists, has early on ambitiously called for a UN-led effort to create a universal and comprehensive Law of Cyberspace[[56]](#footnote-56). Yet, for many reasons a one-shot cyber treaty has not proved to be a realistic option. Fortunately, collective thinking about the necessary processes of cyber strategy has notably evolved. To make a long story short, a new age of cyber diplomacy has begun around 2008 with a manifestly emerging international consensus to concentrate efforts on an alternative to formal treaty-making: the elaboration of confidence-building measures or codes of conduct as normative tools. We may be witnessing a turning point in cybersecurity diplomacy.

The prevailing view is now that CBMs and codes of conduct open a window of opportunity to make real progress towards common definitions and behavioral standards. CBMs have the potential to reduce threat, enhance transparency, make State behavior predictable, are flexible, voluntary, and offer a variable geometry in terms of participants – it is possible to include non-State actors - and follow-up: contrary to coherent treaty-making, participants are free to adopt partial solutions and enact them without delay and independently or with other like-minded stake-holders. CBMs which States embrace do not require ratification; they invite emulation, and are at most – and at best - politically binding. They are thus uniquely suited to foment international consensus-building on an evolutionary scale. A well negotiated package of CBMs with a critical mass of participants may set in motion a process of further incremental change and heightened sensitivity. Clarification of behavioral standards may provide an incentive for going for more.

There are currently many parallel international activities that jointly contribute to consensus-building. Suffice it to cite some. A UN Group of Experts has been instituted in 2011 with the concrete mandate to define “cooperative measures …. including norms, rules of principles of responsible behaviour of States and confidence-building measures with regard to information space”[[57]](#footnote-57) and will report out in 2013. Governments have provided numerous inputs to the Group at the request of the UN Secretary General[[58]](#footnote-58). Their views have strongly supported the idea of identifying CBMs. In a short time, flurries of other national statements to the same effect have surfaced: from Australia, the UK, Germany, at least by implication the US, among others[[59]](#footnote-59). An authoritative academic voice from India has joined the concert[[60]](#footnote-60). China, Russia, Tajikistan and Uzbekistan, reflecting work within the Shanghai Cooperation Council, submitted to the UN Secretary General, in September 2011, a draft international code of conduct for information security[[61]](#footnote-61). Although the document, by virtue of its choice of authors, did not seem to display a sufficient flavor of political correctness, the catalogue of commitments, offered for voluntary subscription by States, should not be disdained. In the meantime, member countries have organized prestigious international conferences, where the CBM idea has been ventilated, and more or less detailed catalogues of CBM contents or contributions to it have figured in the conference summaries (London, Berlin, Beijing, Vienna, Budapest). Apart from the on-going UN exercise, regional organizations are also getting into the act. The ASEAN Regional Forum with its representative membership and participants, 27 nations going much beyond Asia, has zoomed in fully on the CBM theme[[62]](#footnote-62). The OSCE, mindful of its earlier experience with East-West CBMs, is intensively working on a draft code of conduct (see “A Comprehensive Approach to Cyber Security”)[[63]](#footnote-63) and APEC[[64]](#footnote-64), as well as the Shanghai Cooperation Organization[[65]](#footnote-65) are also working on regional arrangements. The Council of Europe, famous for its contribution to a world penal law on cyber crime through the Convention on Cybercrime, has adopted 10 Principles on Internet Governance[[66]](#footnote-66). UNIDIR helps to provide the academic underpinning for these endeavors[[67]](#footnote-67). ONGs in the cyber area, as well as individual researchers offer catalogues of rules of conduct of their own. These catalogues can obviously not be reproduced or analyzed here but provide effective tools for spurring the debate and facilitating CBM negotiations[[68]](#footnote-68). It is to be hoped that the present dynamics in moving to negotiations on such confidence-building measures and codes of conduct be maintained, and that agreement on an appropriate negotiating venue is reached soon.

In order to provide the reader with at least some ideas of content on the current normative endeavors, a brief reference to a short list published by the ITU Secretary General is included:

1. Every government should commit itself to giving its people access to

communications.

2. Every government will commit itself to protecting its people in cyberspace.

3..Every country will commit itself not to harbor terrorists/criminals in its own

territories.

4. Every country should commit itself not to be the first to launch a cyber

attack on other countries.

5. Every country must commit itself to collaborate with each other within an

international framework of co-operation to ensure that there is peace

For the ITU this concise list constitutes the essence of cyber stability and an important part of cyber peace. In the same direction goes the *Erice Declaration* *on Principles for Cyber Stability and Cyber Peace*, (2009) emanating from the World Federation of Scientists, whose list of tenets culminates in the plea “to avoid the use of cyberspace for conflict”. Cyberwar can be avoided, and it should not be considered a legitimate instrument of military conflict. That would go a long way to alleviating the ambivalence of cyber technology, and would sensibly reduce economic preoccupations and economic risks. Cyber peace is the better choice[[69]](#footnote-69).

1. *Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio,* Ministerio de Defensa, Madrid [↑](#footnote-ref-1)
2. Wikipedia, *Cyberwar.* See also Misha Glenny, *Das Ende der Nettigkeiten. Cyberkrieg und Sicherheit im Internet,* Internationale Politik, November/December 2012, p. 80 [↑](#footnote-ref-2)
3. Recent reports about cyber exploitation from China do not only demonstrate the huge and indeed alarming dimension of cyber espionage from that country, but also the great variety of perpetrators: big spying units that steal technological blueprints, negotiating strategies, corporate and government databases from the US in terabyte quantity appear to be part official, part contracted, part independent, and as these studies claim, at least linked with, if not coordinated by a Chinese army unit. This opaque relationship shows a mix of actors and purposes that defies definition and renders the cyberwar notion ambivalent. See David E. Sanger, David Barboja, Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against US,* New York Times, February 19, 2013, and the *Mandiant Report* cited therein and widely commented in other organs. [↑](#footnote-ref-3)
4. Richard A. Clarke and Robert K. Knake, *Cyberwar. The Next Threat to National Security and What To Do About It,* New York, 2010. [↑](#footnote-ref-4)
5. Citable literature with plausible assumptions and calculations is hard to find, but it can be assumed that governments and security institutions dispose of substantiated threat assessments shielded from the public eye. [↑](#footnote-ref-5)
6. It is as yet an open question whether the often-cited Stuxnet virus, a very sophisticated malware, specifically geared to attacking the Siemens-produced dedicated control software (SCADA) of nuclear enrichment installations in Iran, breaks this cascade effect and can be the precursor of smart surgical cyber attacks. In any event, the Stuxnet attacks were not directed at a military installation, and did not emerge in the Internet, but were applied via smuggled flash memory sticks within a plant, thus posing a problem more of physical access control and insider misbehavior. See in this context, James P. Farewell and Rafal Rohozinski, *The New Reality of Cyber War,* Survival, August-September 2012, p.107 [↑](#footnote-ref-6)
7. The cascade effect may be less effective if data – for instance, military data – are managed in Intranets, or if other forms of net segmentation have been installed. Yet, the insulation is only relative, and network defense is always needed to combat the same invisible enemy. The same logic holds with respect to presumed plans of certain countries to opt out of the world-wide Internet structure, creating national digital borders in a “cybered Westphalian age”. Such a national net segmentation will never be complete and finally ineffective. [↑](#footnote-ref-7)
8. Further down more detailed reference will be made to the “Tallinn Manual on the International Law Applicable to Cyber Warfare”, Cambridge University Press 2013, the first comprehensive treatise on the subject [↑](#footnote-ref-8)
9. “it” – Information Technology, Special Issue, 6/2012, p. 255, Manfred Broy, Editorial, *Cyber Physical Systems (Part 1)* München 2012 [↑](#footnote-ref-9)
10. Figures from Portio Research Report Smartphone Futures 2012-2016 [↑](#footnote-ref-10)
11. A more complete list would look to the advancements of nanotechnology, material science, new semiconductor-based sensor technology, the formation and management of virtual systems, new architectural concepts etc. [↑](#footnote-ref-11)
12. For current percentage figures see *OECD Internet Economy Outlook 2012* [↑](#footnote-ref-12)
13. *Symantec Internet Security Threat Report, Norton Cybercrime Report, McAfee Threat Reports.* These reports are issued periodically, and 2011 and, in part, 2012 data and developments are already covered in their latest editions. [↑](#footnote-ref-13)
14. ENISA’s Reports, as recently the *ENISA Threat Landscape: Responding to the Evolving Threat Environment,* of January 2013, stand out because of their broad database, incorporating findings from most other reports, and because of the systematic and definitional analysis of the various types of threats and risks. [↑](#footnote-ref-14)
15. Wikipedia, *Chinese Intelligence Operations in the US;* IISS Strategy Survey 2012, *Intelligence Agencies and the Cyber World,* p. 33. See also Nigel Inkster, *Chinese Intelligence in the Cyber Age,* Survival, February-March 2013, p. 45. See also fn. 3 above. [↑](#footnote-ref-15)
16. The Duqu virus, often cited in the Flame context, also has excellent espionage and data theft properties, but is substantially more complex, possibly related in structure and origin to Stuxnet. Its primary target is also control software like SCADA. Duqu disappears from the affected systems after 36 days which complicates detection. [↑](#footnote-ref-16)
17. Christopher Bronk, Cody Monk and John Villasenor, *The Dark Side of Cyber Finance,* Survival, April-May 2012, p. 129. A specific virus, Gauss, targets financial transactions; there are others. [↑](#footnote-ref-17)
18. Figures from Symantec. Spam may grow less rapidly also because there is increased pressure on spammers; some huge specialized spam botnets having been taken out over the last two years. By contrast, the content of criminal spam has become more sophisticated. [↑](#footnote-ref-18)
19. *Cloud computing: benefits, risks, and recommendations for information security,* November 2009, [www.enisa.europa.eu](http://www.enisa.europa.eu) [↑](#footnote-ref-19)
20. One example is a new technology to segment malware into minute data packets that enter a target system, unrecognized by firewalls and anti-virus systems, but reassemble automatically once inside the host system [↑](#footnote-ref-20)
21. “There is and always will be a permanent race in cyber space between attackers and defenders. Unfortunately, at the moment attackers are one step ahead.” ENISA *Threat Landscape,* January 2013, cited above [↑](#footnote-ref-21)
22. See Javier Candau Romero, *Estrategias Nacionales de Ciberseguridad. Ciberterrorismo.* In: Ciberseguridad, Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, Instituto Español de Estudios Estratégicos, Cuadernos de Estrategia nº 149, Madrid 2010 [↑](#footnote-ref-22)
23. The European Commission through its Vice President Neelie Kroes is currently contemplating to establish a legal obligation for business to report cyber attacks. *News agencies*, 26 November 2012. The EU Commission prepares a Directive in this sense. EU-wide more than 40.000 enterprises would have to submit to the reporting obligation. The initiative has encountered resistance from industry and IT service providers. - ENISA has estimated that 25% of attacks in the EU and the US are not reported to law enforcement authorities. For an initiative calling for voluntary industry reporting, see fn. 55 below. [↑](#footnote-ref-23)
24. www.dhs.gov [↑](#footnote-ref-24)
25. Article in El País and US press, February 21, 2013 [↑](#footnote-ref-25)
26. Cited by Vice President Kroes at the Global Cyber Security Conference, Brussels, 30 January 2013 [↑](#footnote-ref-26)
27. For a summary of the issues, see Jody R. Westby*. A Call for Geo-Cyber Stability* in ITU (Hamadoun Touré and the Permanent Monitoring Panel on Information Security, World Federation of Scientists), *The Quest for Cyber Peace,* ITU, Geneva, 2011, p. 66. In the same publication, see G.A.Barletta, W.A.Barletta, V.N. Tsygichko, *Cyber Conflict*, p. 53 [↑](#footnote-ref-27)
28. For a cautious assessment, stressing the complexity of “line-drawing” in the use-of- force debate, see Matthew C. Waxman, *Cyber Attacks and the Use of Force: Back to the Future of Art. 2(4),* The Yale Journal of International Law, Vol 36 (2011), p. 421 [↑](#footnote-ref-28)
29. In 1999 *Anthony* D, Amato, *International Law, Cybernetics and Cyberspeace,* 76 Intern.Law Studies, p. 59, predicted that “attacks in the Internet will soon be seen as clearly illegal in international law, and customary international law may already have reached that point”, but clearly developments since then have not gone that way. [↑](#footnote-ref-29)
30. See footnote 7 above. [↑](#footnote-ref-30)
31. The Manual also makes clear that not all transfrontier cyber attacks, even though issuing from a state, constitute a violation of the law of armed conflict or international law generally. Thus cyber espionage, in “peace” or armed conflict, does not fall within the purview of international law (except in special cases, e.g. when disregarding the inviolability of diplomatic archives and communications). One of the important elements of cyber conflict, massive intrusion into digital systems for purposes of espionage, an Advanced Persistent Threat, is thus to be judged under *national* cyber laws and sanctions, such as the Budapest Convention defines. [↑](#footnote-ref-31)
32. Barletta, Barletta, Tsygicho, op.cit. p.60 [↑](#footnote-ref-32)
33. A brief list of the various “warfare” modalities has been offered by ITU Secretary General Touré in *The international Response to Cyberwar, in* The Quest for Cyber peace, op. cit, p. 86 [↑](#footnote-ref-33)
34. Another good example for this emerging instinct of prudence can be found in current reports on a draft US Presidential Directive embodying legal rules for the military in defending or retaliating against a major cyber attack, fully respecting International Law The rules will reportedly endow the President with broad powers, including for a preemptive strike, but, given the consequences and the attribution problems, also reflect an attitude of substantial restraint, ruling out “automatic” retaliation, and reserving the prerogative of ordering strikes to the President as Commander-in-Chief. David E. Sanger, Tom Shanker, *Broad Powers Seen for Obama in Cyberstrikes,* New York Times: February 2, 2013. See also Jamie E Condliffe, *Obama Has Signed a Secret Directive to Stymie Cyber Attacks,* Washington Post, Nov. 15, 2012 [↑](#footnote-ref-34)
35. See article of Jody R. Westby on Forbes blog <http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/> [↑](#footnote-ref-35)
36. Examples taken from Westby, fn. above [↑](#footnote-ref-36)
37. If attribution of origin of an economic attack is reasonably certain, some economic counter measures, like discontinuation of relationships, refusal to deliver, withdrawal of trade benefits, or – for a government – withholding of most favored nation status or other punitive trade measures, may be legitimate. Responding to the current surge of cyber attacks on US corporate assets and infrastructures, President Obama has recently spoken of such measures. [↑](#footnote-ref-37)
38. The European Commission, a trailblazer in constructing digital strategies for the 27 members of the European Union, thus unifying their digital policies and defense, is using the “resilience” concept as an overriding finality, for instance by creating – through ENISA – a “European Public Private Partnership for Resilience (EP3R), and placing its recent draft Cybersecurity Strategy of the EU in a major way under the plank “Achieving cyber resilience”.

    [↑](#footnote-ref-38)
39. www.conventions.coe.int [↑](#footnote-ref-39)
40. *Estrategias legales frente a las ciberamenazas,* Cuadernos de Estrategia nº 149, op.cit., p. 116 [↑](#footnote-ref-40)
41. Figures from ENISA [↑](#footnote-ref-41)
42. [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)*.* The TPM is used in the operating systems of most major providers. Trusted Computing does however, face severe criticism from the free software community on the ground that it produces customer lock-in. [↑](#footnote-ref-42)
43. The ITU in its Global Security Agenda is committed to the “Development of strategies for the creation of globally accepted minimum security criteria and accreditation schemes for hardware and software applications and systems”. See also the chapter *Designing for Security* in *Information Security in the Context of the Digital Divide,* Recommendations submitted to the World Summit on the Information Society (November 2005) by the Permanent Panel on Information Security of the World Federation of Scientists, Doc. WSIS-05/TUNIS/CONTR/01 at www.itu.int [↑](#footnote-ref-43)
44. [www.iso.org](http://www.iso.org), [www.iec.ch](http://www.iec.ch). The Spanish member organization of both is AENOR which is also setting standards of its own (in this context see UNE 71502) and provides certification. [↑](#footnote-ref-44)
45. The *Revista Seguridad en Informática y Comunicaciones*, [www.revistasic.com](http://www.revistasic.com), an excellent publication, and certainly the best journal in Spain in the information security field, helps the non-professional reader to keep track of these various distinctions as they are earned by Spanish enterprises. The editor of this journal, SIC, also organizes periodic cybersecurity conferences in Spain. [↑](#footnote-ref-45)
46. These infrastructures are generally understood to include, in the broadest sense, [electricity generation](http://en.wikipedia.org/wiki/Electricity_generation), transmission and distribution, gas production, transport and distribution, oil and oil products production, transport and distribution, [telecommunication](http://en.wikipedia.org/wiki/Telecommunication), [water supply](http://en.wikipedia.org/wiki/Water_supply) (drinking water, waste water/sewage, stemming of surface water (e.g. dikes and sluices), [agriculture](http://en.wikipedia.org/wiki/Agriculture), food production and distribution, [heating](http://en.wikipedia.org/wiki/Heating) (e.g. [natural gas](http://en.wikipedia.org/wiki/Natural_gas), [fuel oil](http://en.wikipedia.org/wiki/Fuel_oil), [public health](http://en.wikipedia.org/wiki/Public_health) (hospitals, ambulance [transportation](http://en.wikipedia.org/wiki/Transportation) systems (fuel supply, railway network, airports, harbors, inland shipping);[financial services](http://en.wikipedia.org/wiki/Financial_services) (banking, [clearing](http://en.wikipedia.org/wiki/Clearing_(finance))), [security services](http://en.wikipedia.org/wiki/Security_agency) (police, military). The energy component is often considered the most vulnerable part. [↑](#footnote-ref-46)
47. COM/2009/149, endorsed by the European Council in Resolution 2009/C 321/01. See also the Directive 2008/114/CE on the Protection of European Critical Infrastructures [↑](#footnote-ref-47)
48. www.tallinnciipeu.eu/?id=conference [↑](#footnote-ref-48)
49. For key findings, see www.enisa.europa.eu [↑](#footnote-ref-49)
50. JOIN(2013 1 final). The Strategy is accompanied by a draft directive on measures to ensure a high common level of cyber protection [↑](#footnote-ref-50)
51. [www.itu.int](http://www.itu.int); www.itu.int/ITU-D/cyb/cybersecurity/impact.html 52 [www.bsi.bund.de](http://www.bsi.bund.de), for the CIIP platform see www.kritis.bund.de

    [↑](#footnote-ref-51)
52. [↑](#footnote-ref-52)
53. *BAE and Vodafone in cyber safety deal,* Financial Times, and news services, 18 February, 2013 [↑](#footnote-ref-53)
54. CERTs since 1990 are coordinating and exchanging information in an informal international organization FIRST; there is room for more effective coordination. Already in 2004 this author has recommend that the CERT approach should not only be universal, but should, beyond individual information processing and assistance, develop a systematic lessons-learnt approach, see Henning Wegener, [*Learning Lessons from Cyber Attacks: Broadening the CERT Framework*](http://www.unibw.de/infosecur/publications/papers_supporting/infosecur/documents/supporting_documents/wegener_lessions_paper_2004), at www.unibw.de/infosecur [↑](#footnote-ref-54)
55. See, for instance, René Obermann, *Uniting for Cyberdefense,* New York Times op.ed. page, February 21, 2013 [↑](#footnote-ref-55)
56. *Toward a Universal Order of Cyber Space: Managing the Threat from Cybercrime to Cyberwar,* Document WSIS-03/GENEVA/CONTR/6-E,, [www.itu.int/dms\_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf),, also at [www.unibw.de/infosecur](http://www.unibw.de/infosecur). See also Ahmad Kamal, *The Law of Cyber Space: An Invitation to the Table of Negotiations,* UNITAR, Geneva 2005, [www.in.int/kamal/the\_law\_of\_cyber\_space](http://www.in.int/kamal/the_law_of_cyber_space). At the United Nations, Russia has as of 1998, in a series of resolutions advocated a Cyber Treaty, proposing to some extent conflictive and probable unimplementable contents, see Res. A/53/70 up to A/65/41. These resolutions had, however, the undoubted merit of keeping the argument alive that a major universal normative effort was required. [↑](#footnote-ref-56)
57. A/Res/66/24 of 13 December 2011 [↑](#footnote-ref-57)
58. A/66/152 and A/66/152 Add.1 [↑](#footnote-ref-58)
59. See previous footnote and the positive utterances at the cyber session of the Shangri-La Dialogue, IISS news July 2012. For Germany, see also “Challenges in Cyber Security: Risks, Strategies and Conference Building, Conference Report, December 13 and 14, 2011, Berlin, [http://www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/ Abruestung/Projekte/ Cybersicherheit.html](http://www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/%20Abruestung/Projekte/%20Cybersicherheit.html).The German Federal Foreign Office, in addition, supports a 2012 UNIDIR project on International Cybersecurity and CBMs [↑](#footnote-ref-59)
60. Arvind Gupta, CBMs in Cyber Space: What Should Be India’s Approach?, IDSA, Institute for Defence Studies and Analysis, June 27, 2012 [↑](#footnote-ref-60)
61. A/66/359. See also the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security, signed in Yekaterinburg on 15 June 2009 [↑](#footnote-ref-61)
62. Secretary of State Clinton at the Pnom Penh ASEAN meeting on July 12, 2012: “This Forum includes some of the world’s largest cyber actors. So this is an appropriate setting for a sustained, meaningful dialogue on cyberspace issues. In the years ahead, we should work together in support of responsible norms and standards, and pursue practical measures to build confidence and reduce risk”. The ARF organizes a Seminar on Confidence-Building Measures in Cyberspace in Seoul next September. In May of this year ASEAN defense ministers called for an ASEAN “master plan of security connectivity”.

    63 www.osce.org [↑](#footnote-ref-62)
63. [↑](#footnote-ref-63)
64. See the APEC TEL Strategic Action Plan 2010-2015, www.apec.org [↑](#footnote-ref-64)
65. No home page in English of the SCO could be detected. News are best gathered from the web pages of the member countries. [↑](#footnote-ref-65)
66. www..coe.int [↑](#footnote-ref-66)
67. UNIDIR, www.unidir.org, organizes conferences and participates in others. Particularly relevant the 2012 conference on *The role of Confidence-Building Measures in Assuring Cyber Stability.* [↑](#footnote-ref-67)
68. For a tentative listing of principles to be embodied in a global code of conduct, see Henning Wegener, *La ‘ciberguerra’ se puede evitar,* Política Exterior, Madrid, No. 146, March/April 2012, p140; from the same author, *Die Diplomatie des Cyber-Friedens, 2011* at[www.unibw.de/infosecur](http://www.unibw.de/infosecur), and also *Regulating Cyber Behavior***:** *Some Initial Reflections on Codes of Conduct and Confidence-Building Measures,* August 2012, The Science and Culture Series, World Scientific, Singapore 2013 (in press)

    [↑](#footnote-ref-68)
69. See also Henning Wegener, *A Concept of Cyber Peace* in *The Quest for Cyber Peace,* op. cit., 2011. In the same publication, the Erice Declaration is also reprinted. [↑](#footnote-ref-69)