A METHODOLOGY FOR MEASURING THE CAPABILITY TO COUNTER CYBERSECURITY-RELATED OFFENSES

INFORMATION DOCUMENT

15 May 2006

NOTE

This report has been written by Professor Benoît Morel, from Carnegie Mellon University, Pittsburgh, Pa 15213. The original purpose of the report was to identify indicators that could be used as a metrics for cybersecurity. The title evolved into a “Methodology for Measuring the Capability to Counter Cybersecurity related Offenses”.

ACKNOWLEDGEMENTS

The material on which this report is based was gathered by more than 80 students (a mix of grad students and undergrads). Several members of CERT contributed to the conceptual framework.

The author wants to thank everybody for his or her contribution. He was somewhat overwhelmed by the amount of information to process and as a result did not do justice to all of it and to the quality of what he was given.

The author takes sole responsibility for the remarks, conclusions and recommendations made in this report.

EXECUTIVE SUMMARY

Cybersecurity is a byproduct of the phenomenal growth of the internet. Concerns about cybersecurity have grown to the point of raising questions about its implication for the long term use of the internet, in particular in the context of the cyberization of developing countries, which is picking up rapidly. Cyberspace has become a dangerous place. Cybersecurity is inherently international and the effort to make cyberspace more secure has to be international.

Cybersecurity is changing fast. The art of cyberattacks has been improving spectacularly over the years. So far cyberdefense has more or less been able to improve sufficiently to keep the damage due to malicious activities in the internet within acceptable limits. Nothing guarantees that this situation will last for ever.
Cybersecurity is also inherently complex. It is based on the malicious exploitation of technologies (software and hardware) that few understand fully. One of today's challenges is to put the basis for an international cooperation on cybersecurity. This begins with coming to grips with the vast world of cyber-offenses and no less confusing world of how to counter them.

In this report we wrestle with the difficulty of developing indicators or other methods of assessing the adequacy of cyberdefenses in the context of the changing world of cyberattacks. Developing good indicators would be a major contribution at a time where developing countries are getting more cyberized. If they fail to take cybersecurity seriously at the beginning they will later, but after having suffered the consequences of their original mistake. For them it is a case of pay now or pay later.

A large portion of this report is based on reviewing the situation in developing countries how their cyberization affects the general equation, what kind of paradigm they can follow to build their own cybersecurity national capability and the kind of challenges they will have to overcome.

On the one hand cybersecurity concerns every nation without exception. On the other hand each nation is a particular case. This is one among many reasons why building indicators informing on the state of readiness of different nations is difficult if not futile.

Among the other reasons is the fact that the knowledge in cybersecurity is scattered and the most useful part of it is not easy to access. Scholars for example are not as good experts as system administrators in implementing efficient defense systems in practical circumstances. This expertise is essential. Hackers use their imagination differently than the engineers. As a result they find ways to exploit vulnerabilities faster and better. Many exploitable vulnerabilities are due to the way systems are configured or implemented. They are not inherent in the design of the system.
What makes cybersecurity so challenging is partly because security was not a prime preoccupation when the internet was designed originally. The internet today has some really serious vulnerabilities (like the Border Gateway Protocol) that will not go away and that will not be solved through superficial fixes. But the internet has become a very large international infra-structure. Any radical change of hardware or protocol will be difficult to implement. The more the use of the internet intensifies, the more difficult this will be.

Failing to come to grips with all these issues could have dire consequences. The art of cyberattack is evolving in a variety of way. One is the possibility of attacks involving many computers (thousands to millions). Some of the cyberattacks of tomorrow may dwarf what we have seen so far.

TABLE OF CONTENTS

page

EXECUTIVE SUMMARY

1 PROLEGOMENA: THE NATURE OF CYBERSECURITY 3
- **1.1** The different levels of cybersecurity 3
- **1.2** The four different faces of cybersecurity 4

2 ON THE DESIRABILITY AND DIFFICULTY TO DEVELOP USEFUL INDICATORS FOR CYBERSECURITY-READINESS 5
- **2.1** A challenge for governments 5
- **2.2** Diversity of situation 6
- **2.3** ICT development and cybersecurity 7
- **2.4** National cybersecurity agencies (CERTs as panaceas?) 7
- **2.5** The international nature of cybersecurity has many facets 7
- **2.6** The economics of cybersecurity 8
- **2.7** On the futility of "indicators" 8
- **2.8** About "best practices" 10
- **2.9** What indicators do not capture and should 10
- **2.10** On the difficulty to base any cybersecurity analysis on solid facts 10

3 A BRIEF HISTORY OF CYBERCRIME AND THE CYBERTHREAT ENVIRONMENT 11
- **3.1** The past 11
- **3.2** The present 12
- **3.3** The future 14

4 THE INTERNATIONALIZATION OF THE DYNAMICS CYBERATTACK/DEFENSE 16
- **4.1** Co-evolution between cyberdefense and cyberattack 16
- **4.2** Internationalization of the problem 17

5 GLOBAL CYBERIZATION AND THE CHANGING CYBERSECURITY WORLD MAP 24
- **5.1** Multi facets of cyberization 24
- **5.2** The forces of cyberization in developing countries 25
- **5.3** The contrasts in the cultures of cybersecurity 26

6 THE CHAOTIC WORLD OF NATIONAL CYBERSECURITY SYSTEMS 26
- **6.1** The US example 26
- **6.2** Lessons for developing countries 28
- **6.3** Cooperation between national cybersecurity agencies and regional agreements 28

7 ANATOMY OF A NATIONAL CYBERSECURITY CAPABILITY 33
- **7.1** Every nation is a special case 34
- **7.2** Challenges 36

8 CYBERSECURITY METRICS 37
- **8.1** Three "obvious" indicators 38
- **8.2** Technical indicators 38
- **8.3** Preparing for the future 41

END NOTES

1 PROLEGOMENA: THE NATURE OF CYBERSECURITY

Up until recently, cybersecurity was treated as a nuisance, a by-product of the incredible success of the internet. We are entering in a new era where cybersecurity will influence the future of the internet. Future reforms of the internet will be motivated by cybersecurity concerns.

For governments, cybersecurity is bound to become a formidable challenge, much more than has been the case so far. A good national cybersecurity policy will become a necessary ingredient for prosperity. Establishing a good cybersecurity policy is already difficult at the level of firms. Cybersecurity is complex and it is not yet well understood.

Cybersecurity can be approached from at least two different perspectives (who is affected and how), each time in four different ways:

- cybersecurity can be seen in four different level: individual users, organizations (private and public), technical experts and government policies.[1]
- cybersecurity has four different faces. It can be viewed as an IT security issue, an economic issue, a law enforcement issue or a national security issue.[2]

1.1 The different levels of cybersecurity

1.1.1 Individual users

Cybersecurity affects every netizen. He or she is at the same time potential victim and security hazard. What is expected from individual users is unprecedented complex in telecommunications. Education is often advocated as a crucial part of the answer. In practice people learn probably more by suffering attacks and learning the hard way. Over time one should expect that the level of common expertise in cybersecurity will improve. The deployment of wireless technology has recently documented again the fact that people are prepared to expose themselves more than they know by purchasing an access point, without any protection against use by outsider[3], sometimes at their peril. Voice over IP is perceived as providing a new channel for long distance voice communication cheaply and may very well become also an opportunity for hackers to have a filed day at the expense of gullible netizens. For a long time we will be in the present situation where people will take risks they do not appreciate, will fall for a variety of forms of social engineering such as phishing, credit card companies will have to self-organize themselves to avoid the consequences of individual incompetence and its exploitation by clever criminals.

1.1.2 Organizations

The life of organizations, private or public has been revolutionized by the internet. If for an organization, cybersecurity was merely ensuring the confidentiality and integrity of information within a private network, this would already not be a trivial problem. The system administrator would already have to deal with insider attacks, disgruntled employees. The fact that there is hardly one organization whose the network is not connected with the internet adds a new dimension. Through e-mail and access to websites, a lot of malware and malicious activity can find their way within the network. The fact that most organizations (in particular commercial) have websites complicate further. When the website is in fact an important part of the life of the organization, then the system administrator has to worry about Distributed Denial of Service (DDOS), in addition of having to be involved in security policy, patch management, and the monitoring of the (in general huge) traffic moving inside the network.

The cybersecurity of organizations such as hospitals, drug manufacturers or banks raise special concerns. Hospitals tend to be increasingly cyberized and also increasingly targeted. The cyberthreat is on the confidentiality of data of patients as well as potentially interference with the treatment of electronically monitored patient with potential lethal consequences. Drug manufactures is increasing cyber-controlled. A hacker could potentially remotely modify the proportions of ingredients, for example. Banks are “juicy”

targets and many have been put into situations of extortions. It is believed that banks do not report all the losses due to cyberattacks. Banks cannot rely on a lot of public help against the cyberattacks they are under.

1.1.3 Technical experts

There are in fact at least two kinds of “technical experts”: the hackers and shrewd cyberattackers and those who study cybersecurity as scholars or as system administrators. Not only are their goals different, but so are what they see at the major issues in cybersecurity.

There is an asymmetry of situations between cyberattackers and cyber-defenders. In cybersecurity, the initiative belongs to the attackers. Cybersecurity is very complex, there are many ways a cyberattack can be waged. The attacker needs to find only one hole. The defender in principle has to block all of them.

Attackers use their imagination to make an always more efficient and intelligent exploitation of the almost infinite spectrum of possibilities that computers offer. From one generation of cyberattack to the next we can see a progress, sometimes spectacular toward the design of increasingly complex and large scale attacks. Looking at cybersecurity from the perspective of attackers is as exciting as it is daunting when one takes the perspective of the defenders.

Technical experts also get increasingly well organized. Thanks to institutions such as CERT among others, effective responses to new threats come much faster. But the stakes are increasing.

1.1.4 Government policies

The huge and unforeseen success of the internet is attributed partially by the fact that its growth was unhindered by the government. Cybersecurity and the internationalization of the internet have created a new situation. Cybersecurity was not a preoccupation when the protocols and technologies underlying the internet were developed. One result is to have made cybersecurity a complex problem, almost inextricable. One lesson is that security is not something one adds at the end. It has to be part of the design.

Whereas cybersecurity can be seen as a byproduct of the growth of the internet, it will be a major factor in the way internet will be reformed and organized in the future. The forces that drove the development of the internet were a pursuit or technological excellence through the IETF/RFC process and commercial opportunities. The fact that security will be a more central preoccupation implies a change in the governance of the internet, involving a larger role for governments.

So far government policies have dealt mostly (and with mixed success) with e-government, protecting government assets and systems and the like. In the future, working at creating conditions of a more cybersecure world will be added. However hard governments may find to ensure their own cybersecurity, what they will have to do in the future will be significantly more challenging.

1.2 The four different faces of cybersecurity

1.2.1 An IT security issue

In that perspective the accent is on Information Assurance and Internet Security. Policies deal with countering cyberthreats through firewalls, antivirus software, patching management, intrusion detection, cryptography, network security to counter the threat due to the exploitation of software vulnerabilities, the spread of malicious software (malware) such as backdoors, trojans, viruses and worms and the perceived threat to privacy, among other concerns.

1.2.2 An economic issue

Ensuring that e-commerce, e-finance and the business in general benefit fully from Information Communication Technology (ITU). The big concerns (in random order) are: DDOS , worms and botnets are

of concern, penetration of private networks, hackers/crackers, key logging, industrial espionage, extortions, integrity of data such as credit card information, secure transactions over the internet, copyright issues and intellectual property (IP) concerns, spyware, adware, spam and other abuse of that media either to profile excessively customers or to annoy them, social engineering in general, phishing, pharming, information leaks (information is central to wealth creation in modern society).

1.2.3 A law enforcement issue

What constitutes a cybercrime? How is it defined in different countries? Is there a basis for a sound collaboration among nations to prosecute cybercriminals worldwide for misdeeds they committed against one country from another one? Have all countries the ability to help trace back expeditiously attacks which went through several nations? Are cybercrime being prosecuted in all nations? Are there safe haven for cybercriminals? How does the internet as a medium of communication among criminals and as a medium to conduct criminal activity change the relation between law enforcers (such as FBI) and the population? The internet facilitates the circulation of information illegal in some countries (child pornography in the US, some political statement in China, for example), triggering some response from each government made difficult to implement by the international nature of the medium. The US has instituted laws such as Sarbanne Oaxley ("SOX") which requires private companies to stores their financial records in such a way they can be used in audits and make cheating more difficult. This apparently had a significant impact on the life of the private sector in the US and wherever this law is de facto enforced.

1.2.4 National security issue

The mission of agencies such as DHS, is to focus on that subject. From the threat of cyberterrorist attack, the danger (or lack thereof) of a cyber Pearl Harbor, to the cyberization of our critical infrastructures, cybersecurity has entered the realm of national security concerns. The Chinese openly emphasize the military importance of cyberattacks and information warfare. The government relies on cyberspace increasingly for its activity as well in its relation with the US citizens, to the point of being in danger of not being able to fulfill properly its responsibilities if the internet became dysfunctional. The internet has become a critical infrastructure competing in importance with the electric power grid.

2 ON THE DESIRABILITY AND DIFFICULTY TO DEVELOP USEFUL INDICATORS FOR CYBERSECURITY-READINESS

2.1 A challenge for governments

Cybersecurity concerns all nations without exceptions. But it affects them very differently. No nation is totally safe. Some like the US are more exposed than others. The cyberworld would be a bit more secure if all nations are more or less operating at the same level of knowledge in cybersecurity and were cooperating fully in trying to make cyberspace as secure as possible. This is far from being the case today. The "level" of cybersecurity savvy differs widely between nations. This difference is a source of problem as less secure nations (which tend to be developing nations) can be a source of harm to the other nations, like being a haven for cyberattackers. Developing nations will not enjoy the full benefit of ICT if they do not take cybersecurity seriously.

Governments so far have had a limited role in the life of the internet (this may be one reason for its spectacular success), but cybersecurity is putting an end to that situation and forcing a fundamental change in the role of governments. Security has a law enforcement component that requires the direct involvement of governments.

Because of its complexity and ramifications in so many aspects of the life of modern societies, cybersecurity is bound to challenge governments. In a sense governments today tend to be cybersecurity challenged. They

have an obvious difficulty to find their way in this technology intensive world, with its economic and national security implications.

An additional complication is that cybersecurity is the opposite of static. It changes with time but it will stay as a problem for the long term, an evolving problem. Cybersecurity calls for an adaptive policy to be updated regularly. It is difficult to imagine laws going to the heart of cybersecurity which do not run the risk to stifle our ability to adjust to its changes.

Finally what may be the most difficult challenge for governments is that cybersecurity is so intensely international. Today governments are satisfied with what some sometimes consider a high level of cooperation. The pressure of circumstances and the need to internationalize the response, will probably force the governments to engage in a much higher level of cooperation than they are prepared to contemplate today.

2.2 Diversity of situation

There is a huge diversity between nations as to their degree of cyberization today. This has implications for their cybersecurity.

- In advanced cyberized nations like the United States (US), cyberization affects basically every aspect of the life: from the future management and control of critical infrastructure such as the power grid, the life of hospitals, the life at home of senior citizens, the monitoring of the functioning of appliances such as elevators, etc… Cybersecurity in nations like that has reached a very high level of maturity and complexity and is getting more complex by the day.
- By contrast, many developing nations are at an early stage of cyberization. The internet penetration is minimal to small (less than 10%). The internet connection has relatively low capacity and it is used mostly for communication (e-mail) and access to websites. Most netizens do not use their own personal computer. They tend to use internet cafés instead. Those nations tend to offer much less targets to cyberattacks, as few of their assets are exposed. On the other hand those nations fall prey to viruses or worms easily. In those nations, there is scarcity of technical expertise. The best computer experts are often the cybercriminals.
- Some nations have an intermediary degree of cyberization (> 10% internet penetration) or are in the process of cyberizing themselves. In some of them cyberization is the result of a pull from their government to promote ICT projects as a driver of economic prosperity. In most nations there is an even bigger push from the population to increase access to the internet. In most (if not all) of those nations, the process of cyberization is not accompanied by an adequate concern for cybersecurity.
- Cyberization can mean the connection of many new netizens, either with their own computers or through shared computers in institutions like Internet cafés. Hackers are among the first to use the internet. This may explain why in the early stage of the internet penetration in a country, the proportion of hackers and cybercriminals is relatively high.
- The internet provides access to assets in any country to hackers from any other country. In a world filled with huge economic inequality, a clever hacker can hope to outsmart rich users and steal some of their assets. The protection of financial assets has become a very complicated proposition in particular where so much relies on the savvy of the owners of the asset. As a result the internet has become a favorite conduit for international crimes. The process of cyberization of developing countries by increasing the number of savvy hackers exacerbates this problem.
- In 18 years the art of cyberattack has improved spectacularly. But it would be wrong to assume that the state of the art of cyberattack today will not improve further. In fact it is still improving at the same rate if not faster. The art of cyberdefense is following as fast as it can. Cyberdefense is reactive by nature. In that arms race, the strategic advantage belongs to the attackers.

2.3 ICT development and cybersecurity

Cybersecurity is an important component for the success or failure of ICT projects. Experience has shown abundantly that neglecting this factor or planning to add cybersecurity late in the project, or at the end, or as a reaction to some attack, are dangerously flawed approaches. Cybersecurity has to be part of the design from the beginning of ICT projects. There is in principle an element of complexity as it would be as counterproductive to overestimate the importance of cybersecurity that underestimating it. Cybersecurity is vital for the success of ICT, but it should not be its organizing principle. If it is true that the benefit of ICT can be erased through cyberattacks, one must remember that cybersecurity merely contributes to the success of the project, it is not the origin of the benefit for the ICT project. But today, we are nowhere close to face this dilemma. Today the problem is complete absence of awareness of the problem in most of the governments involved as well as the World Bank for example. Considering the active resistance met by those who tried to alert those parties, it seems that the resolution of the UN resolution calling for a "culture of cybersecurity" fell in deaf ears and that only a cyber-fiasco of significant proportion will do the job.

2.4 National cybersecurity agencies (CERTs as panaceas?)

Some countries are aware of the need for cybersecurity initiatives and in some cases have some. The instinct is often to create a national "CERT". This approach met with success in some cases (Australia and Brazil among others and in their different ways qualify to be successes). Some nations try to get help for that. They tend to look at the US in general and American CERT in particular for inspiration. Some nations have CERTs or equivalent institutions. Others do not. CERTs need not be government institutions. Large companies and agencies (such as ministries) have their own CERTs. CERTs tend to belong to the Forum of Incident Response and Security Teams (FIRST). FIRST has over 170 members, few are national CERTs. Membership comes at a price and provides a network of contacts. The impact of FIRST on cybersecurity worldwide is certainly not negative. But one may question whether FIRST makes a significant difference.

The US is probably the most advanced or cyber-savviest nation today. One can understand why it is used as inspiration. But when it comes to cybersecurity, the US is as complicated as it gets. There is not one well defined, coordinated and coherent US cybersecurity policy. The world cybersecurity in the US is made of many institutions, agencies, consortia and organizations, many but not all for profits. The institutions underlying the cybersecurity response in the US build a self-organized system which has never part of a plan. To a certain extent, the situation is similar in "advanced industrialized" countries such as the UK, Switzerland, Netherlands, Germany, France, Japan, Korea or Australia. But despite the similarity in the level of cybersecurity, the way it is accomplished differ significantly between these countries. In each of these countries what constitutes the cybersecurity policy is the result of a self-organization around perceived needs and also situation and culture. The institutional structure dealing with cybersecurity is influenced by these differences of approach or attitude. For example: "In France, cybersecurity is seen both as a high-tech crime issue and an issue affecting the development of the information society."[4] In Australia cybersecurity is "part of the overall counter-terrorist effort"[5].

For developing nations in the process of cyberization, there is no model to follow. On the hand, whatever knowledge and expertise there is toward designing a national cybersecurity policy can be found in those nations and in particular in the US. But this expertise is not concentrated in one place. It is distributed in among other places, private entities. The American CERT/CC (which is somewhat distinct from US CERT), has done its best with limited means to provide as good quality help as possible in setting up national capacities. But this is not a trivial proposition: CERT in the US is not a national agency[6] coordinating the cybersecurity policy of the US government, what the national CERTs try to be. Secondly the legal, social and political contexts are different and this affects the design of the national CERTs and complicates the work of those who want to help as they have to analyze and adjust to this different reality. Receiving structures to help developing nations seeking help and advice have to be developed. The setting up of adequate national agencies to coordinate the cybersecurity of newly cyberized nations is work in progress.

2.5 The international nature of cybersecurity has many facets

Cybersecurity is international in more than one way. Originally an American technology, the internet is now an international infra-structure. There are far more netizens outside of the US than inside. The internet itself

is an international critical infra-structure shared by all nations. There has been recently a growing realization that the basic make-up of the internet may have to be revisited. As it is the internet is a passive pipe through which malicious activity can pass and coming from anywhere in cyberspace can reach any individual, organizations, government agencies or critical infrastructure. Is it possible to make the internet as infrastructure more actively part of the solution. In a limited way this is happening as in some countries, Internet Service Providers (ISPs) offer their clients limited protection against malware such as viruses and worms, for example. A closer look at the internet as an infrastructure reveals that however passive it may look it is in fact a sophisticated infrastructure, which carries packets from one end of the world to the other through many hops sometimes and reliably and fast enough to have inspired the development of Voice over IP. The routing system (which in fact is based on the so called Border gateway Protocol, BGP) is efficient and sophisticated as is the system of Domain Names (DNS), which is a very large distributed library. But both BGP and DNS are also mega liabilities in an environment involving a lot of malicious activity. Both could be attacked with devastating consequences for the internet traffic. The internet is mostly privately owned (by ISPs). There is an ecology of ISPs. A few are very big and tend to be transnational. Many (in the thousands) are significantly smaller, and in some nations, they are controlled by the government.

If the basic protocols underlying the internet and its fundamental architecture had to be reconsidered, what would be the right forum for that? The same kind of people as the team of self-appointed computer nerds which put together the previous protocols? This seems improbable. Considering that a problem as apparently simple as a system of assignment of IP addresses can degenerate into an intractable source of international controversy, even the most well-intentioned mind will find it difficult to be optimistic about the ability of the international community to tackle really complicated problems like the new generation of Internet protocols.

2.6 The economics of cybersecurity

Cybersecurity comes at a cost. The economics of cybersecurity is far from understood, but it is clearly not a negligible factor. The international dimension of that problem has not yet reached the radar screen. Since cybersecurity affects nations differently, if and when they begin to take cybersecurity a bit more seriously, the issue of money may become more prominent. Rich nations will find in their vested interest to see poor nations putting adequate resources for measures more relevant to the rich than the poor. But this is a problem for the future. Today we have not yet reach the point where the governments of most developing nations have realized the importance of this subject.

Cybersecurity is not only a technological problem, it is steeped in technology, but first and foremost a human problem. The criminal opportunity is created by the technology and its use, but cybersecurity is the result of a malicious exploitation by human beings of those opportunities. Cybersecurity therefore should be discussed within the cultural, economic, social and political context in which it leaves. Easier said than done.

As we report later, the geographic distribution of hackers and cybercrimes is not uniform, as if it reflected the cultural, economic or social diversity of our world. It is a simplification, but not outrageous to state that to a large extent the huge gap of standards of living between the few rich countries and the many poor countries plays an important role. On the one hand the increase in the use of the internet for banking and e-commerce seems irresistible in rich countries. It gives added opportunities for clever cybersavvy otherwise much poorer netizens of developing countries to use their skill and imagination to pilfer what they may consider excess wealth. Furthermore they do that remotely with a realistic hope of not being caught.

The growth of the internet is taking place in a world of globalization. It is an agent and a product of globalization. Cybersecurity is emerging at a time of globalization of what used to be more local conflicts. Terrorism is a well-known one. Whereas the world has not yet seen any cyberterrorist act yet, many possible ways to inflict terror by cyber means exist on paper, and may one day occur. The threat of such contingencies belongs to a discussion of cybersecurity. Entangling terrorism to the already inextricably complicated world of cybercrime and cybersecurity is bound to add another degree of complication.

2.7 On the futility of “indicators”

Is it possible to put some intellectual order in the confused and confusing world of international cybersecurity? Is it possible to identify cybersecurity “indicators”?

Cybersecurity "indicators" to be useful, should talk to this complicated international situation. They have to be such that when applied to a given country or problem, they reveal useful aspects or suggest corrective actions. The goal of this paper is to develop a methodology to make such assessments. The first question is what methodology will we use in this work to develop such a methodology?

Are there good indicators of cybersecurity maturity or readiness? What do we expect from indicators? The short answer is that they should help calibrating whether a nation present cybersecurity hazards that other do not. We distinguish between two types of indicators: direct ones and indirect ones.

2.7.1 Direct indicators

- Is there a mechanism of enforcement of "best practices" or an effort to spread a "culture of cybersecurity"? How does the information about cybersecurity spread in the country?
- Are there national CERT or CSIRT organizations or some private or public substitutes? Relation between CERTs, CSIRTs if any, and the government and private sector.
- What constitute a cybercrime in that country? Are there cybersecurity laws punishing some cybercrime? What is the record of prosecution of people?

2.7.2 Indirect indicators

- How is the government involved in the Internet? Does it try to promote safe e-commerce and e-finance? Does it use the internet as a law enforcement mechanism by spying of citizen? Does it ignore the internet altogether? Does it see cybersecurity as a law enforcement problem, and economic problem or otherwise? Does it take the problem seriously?
- Is e-banking, e-government practiced in that country? Level of e-governance: does the government uses website, and the internet for itself or for official interaction with citizens?
- Are there large private networks, and who owns them?
- How does visa (credit card) operate? Is the PCI standard a "de facto standard" enforced in that country?
- Are the infrastructures cyberized or in the process of being cyberized? (i.e. is there a national security dimension in cybersecurity?)
- How much resource is the government prepared to put for cybersecurity? What organism, agency or ministry (ies) are in charge of the cybersecurity?
- Do a lot of spam and malware seem to originate from that country? (Costa Rica for a while was ostracized because too much spam was originating from there. Bulgaria was nicknamed "virus factory". China has been accused of letting hackers operate from their territory, as if the "great firewall of China" was a one way barrier only).
- Are the ISPs independent operators or under the control of the government? (The fact that the government controls does not imply that the place is cyber-insecure. But it affects what is possible and not)
- How good is the internet connection with the rest of the world: does it go through space and satellite, or does it involve a connection to submarine cables? How many connections are there? (Pakistan recently was crippled for a few weeks because it sole connection to submarine cable became partially dysfunctional).
- What is the record of internet incidents in the country and how well they were resolved? How robust is the ICT infrastructure? (Russia had a serious down in Moscow recently which affected a location with many servers at the same time).

This is the kind of "indicators" which reflect more or less the state of the cybersecurity culture today. Many of them can be questioned on several grounds, and some may suggest other indicators. Some would suggest

using the degree of use of Network Address Translation (NAT) a proxy for the number of protected private networks as an interesting indicator. This would be an indirect measure of maturity. For a developing country in the early stage of cyberization, one does not expect a high degree of NAT. On the other hand useful indicators would tell whether the country is on its way to be a worldwide problem case and dangerous for itself, or the opposite.

2.8 About "best practices"

The concept of "best practices" is somewhat controversial as is its validity as a cybersecurity indicator. It is also emblematic of a common tendency of trying to oversimplify cybersecurity. A bit like what Einstein said about mathematical models, cybersecurity should be made as simple as possible, but not simpler. One problem with cybersecurity today is that we do not know how to simplify it safely. We still have to learn to do that.

"Best practices" in cybersecurity are not arbitrary rules. It would be as silly to ignore or disregard the idea of "best practices" as it is to believe that they provide adequate protection against cyberattacks. At best, they can reduce their probability and mitigate their effect. They are not a rigid set of well defined rules. What is referred to as "best practices" changes with time. The most valuable criticism against letting best practices play an important role is that it tends to lead to excessive dogmatism in a situation which requires intelligence and flexibility. Managing the security is too complex to be reducible to compliance to rules, which are the same for all. What we see sometimes is that too much attention put in concentrating on best practices at the cost of performing the more complex job of managing security less well. In the context of developing countries, it is very difficult to see what they entail and how well they can be enforced.

2.9 What indicators do not capture and should

When applied to most of the countries of the world those indicators fail to help to significantly inform on the state of cyber-advancement of the world. What a quick survey of the world taught us is today's world map of cybersecurity is littered with anecdotal realities, difficult to capture into "cybersecurity indicators", but which will probably determine the future of the cyberworld.

According to David Finn, Microsoft's director of digital integrity for Europe, the Middle East and Africa, counterfeit centers are shifting from California and Western Europe to countries such as Paraguay, Colombia and Ukraine.

We also learned that in 2002, 20 percent of the total numbers of credit card transactions in Indonesia on the Internet were cyberfrauds. Most of those Credit Card frauds were done from Warnets (Indonesian Internet Kiosks) and most Warnets are facing a very difficult time to survive as viable businesses. As a result some of them are turning to crimes related to "carding" (credit card fraud, sales of expensive items, etc).

Nigeria, with 1.1 % has a low internet penetration by African standards (2.5% in average), but it is also the 3rd highest in the world for the number of cyber fraud perpetrators. It accounts for 2.87% of worldwide perpetrators[7].

In developing countries cyber-regulations, when they exist at all, tend to be vague making it difficult to prosecute resulting in few convictions and the convicted being lightly punished. Despite the poor state of connectivity in the country, Tanzania is an appealing place for a cyber-terrorist to operate, since there does not seem to be any good legal instrument to prosecute them. While officially Nepal (the 14th poorest country of the world) is officially enforcing intellectual property laws, local bazaars sell pirated software and the government is one of the best customers… An internet café opened in 2003 at base camp of the Everest… That could be an attractively exotic place to launch a cyberattack.

2.10 On the difficulty to base any cybersecurity analysis on solid facts

We are very aware of the fact that many computer crimes are not detected and even when they are, more often than not they probably are not reported. Any cybersecurity analysis is unavoidably based on a biased sample with a lot of missing information. Having this caveat in mind, we believe that one of the messages of our survey is that in the world of today, the really important cybersecurity issues are related with the present

state of cyber-anarchy to a certain extent caused by and certainly amplified by the cyberization of developing nations. This has created a situation of unprecedented complicated danger for the short term and a need for an international response to define. So we decided to use our survey of the different countries of the world as a basis of our analysis of the state of cyber-anarchy of the world and in the hope of eliciting the basis for an international response.

3 A BRIEF HISTORY OF CYBERCRIME AND THE CYBERTHREAT ENVIRONMENT

3.1 The past

The concept of cyberworms or viruses comes back a few decades. But it was the release in 1988 of the RM Morris worm that made cybersecurity a subject of concern. R.M. Morris was a graduate student in Cornell but he released that worm from MIT. The worm was a self-propagating malicious code, finding its way in computers by exploiting a buffer overflow vulnerability in a unix program. The speed at which the worm spread in what was the internet then caught Morris by surprise and as a result the internet was so clogged that he had no way to inform the people trying to control the worm, of what to do…

This episode convinced the US government to create a center to coordinate a response to that kind of contingency. CERT, the Computer Emergency Response Team was born the same year, in 1988.

From then on, malicious activity on the internet began to be analyzed and victims had a place to call for help. In the first years, the most common cyberattacks were against passwords. Malicious programs called Trojans appear soon. Trojans are codes one download unwittingly while downloading other software. When inside the infected computer, Trojans install themselves. Typically they are designed to provide remote access to hackers to the computers.

Trojans can be key loggers. In that case they log the key strokes and sent the information away. In that information are user ID and passwords among other things. This is used for example to access bank accounts.

The Morris worm exploited buffer overflow vulnerability. It took a few years before this kind of exploit entered the arsenal of hackers. This happened with the publication in 1996 of a detailed description of how to do exploit a buffer overflow vulnerability, by a hacker nicknamed Aleph One.[8]

Although today common practice, the exploitation of buffer overflows vulnerability was slow to catch, partially because it is not completely trivial to do. When done successfully, it gives hackers administrative control on computers and servers. Buffer overflows vulnerabilities occur in programs written in C or C++. A buffer overflow takes pace when one tries to put in a buffer more than it can contain. The effect typically is to make the program crash. But if the hacker understands well the architecture of the processor (i.e. if he or she knows how to reach the return address) he or she can fine tune the overflow in such a way that he or she can take control of the computer. Writing a buffer overflow exploit is not trivial. When the first buffer overflow exploits were made, several weeks would separate the moment a buffer overflow vulnerability was detected and the appearance of the exploit. Now that can take less than a day.

It turns out that most of the commercial software possess exploitable buffer overflow vulnerabilities. Vendors in general produce patches as protection against the vulnerability that they distribute for free. Patches are not a panacea. They sometimes affect (in general negatively) some functionality in the program. Although this is rare, they sometimes introduce new bugs. But they are pieces of code that can be reverse engineered by hackers. Paradoxically patches give clue to hackers by helping them figuring out exploits against the vulnerability, which allow them to attack unpatched computers. Buffer overflows is by far the single most exploited vulnerability by hackers.

The mid nineties also witnessed the emergence of the so-called Distributed Denial of Service attacks (DDOS). The idea is to deny access to a website by making so many queries that it saturates the site. Many computers are needed so DDOS go in two stages. In the first phase, “zombies” are deployed. Zombies are Trojans somehow introduce into many computers. They are programmed to stay dormant up until they all

wake up at the same time to launch the second stage of the attack. In the second phase, all the zombies overwhelm a target with more synchronous queries than the victim can accommodate. Under this kind of attack, in 2000, websites such as Yahoo, eBay or Amazon.com were inoperational for several hours. They lost a lot of money. Against that kind of attack, no good protection is known to day. Filtering the malicious traffic would be a nice solution if it were a realistic option. But in general the attackers spoof the source address of the malicious traffic which as a result is very difficult to distinguish from the legitimate traffic. Another possibility would be to lease at very high price extra webspace to companies like Akamai. Then it becomes difficult for the attacker to have enough computers firing to prevent the legitimate traffic from reaching the website. But the price is high. So this is worthwhile solution only for a certain class of websites. DDOS has become a very common form of attack.

3.2 The present

Modern attacks tend to use the same kind of concepts as the attacks of the recent past, but at a larger scale or in more shrewd ways. Modern attacks are frequent. Due to the use of automated tools among other things, a computer does not need to be connected to the internet for more than a few minutes before it is port-scanned for example. Cyberattacks most of the time begin with a port scan, which informs of which port is open, before going to the second phase of identifying the operating system or checking the presence of a vulnerability. Some worms immediately queries some port to check whether a specific exploitable vulnerability is present.

3.2.1 Modern worms

Some of the new cyberworms spread faster than our ability to do anything about them before they have infected most of their potential victims like stopping them from clogging the internet. They are referred to as “flash threats”. The first one appeared in January 2003 (Slammer or Sapphire). Since a few more have appeared. Flash threats have made even more exposed further the limitations of today’s intrusion detection capabilities. Slammer infected 90% of its victims worldwide in about ten minutes. Worms propagating much faster are conceivable. Scenarios of worms spreading world wide in seconds or less exist on paper[9].

To counter that kind of threats automatic detection is a necessity, as well as a response which does not require a man in the loop. Today we are far from such a situation. New virus or worms are detected by human beings and because of the effect of their infection. Antivirus software can detect only malicious codes like viruses or worms which have already been released before. Detection of new malicious codes (such as anomaly detection) is far from being a perfected art and exists only in labs.

Antivirus software do not provide protection to malicious codes they encounter for the first time. They alert the users of most of the infections like viruses, worms and other malicious codes after they have been detected and analyzed.

3.2.2 Spam and phishing

There is no equivalent of antivirus software against spam and phishing, which may be today the two forms of attacks that netizens are the most exposed to. Spam has become such a serious source of financial loss and aggravation that it has inspired an international campaign under the intergovernmental antispam pact.

Phishing can be very sophisticated, and when successful can ruin the life of innocents. Phishing pits cybercriminals from anywhere against gullible netizens. The cybercriminals can come from developing countries, while the typical victims are average defenseless citizens of rich countries. They are like low hanging fruits to the much less rich but much shrewder phishers of developing countries. The number of those phishers is growing fast with the internationalization of the internet, compounding a problem not easy to address in the first place.

3.2.3 Spyware

Spyware are sometimes considered as among the worst threat today. According to a survey conducted by AOL and the National Cybersecurity Alliance, in 2004, more than 90% of computers had some sort of spyware.[10] Spyware are programs which record the activity of a computer. Typically this could be

information on sites visited that is use to profile the user for commercial purpose. The goal could obviously be quite different.

Whether a spyware is always a malicious code is unclear. Kazaa (which has been downloaded by more than 215 million times), can be construed as a form of spyware. This observation made the security Computer Associates calls Kazaa the "biggest spyware threat on the internet"[11] .

Spyware is a vast world of software unequally malicious. Under one form or another, infection by spyware is very common in computers. When the statistics is restricted to malicious spyware, numbers vary and so does the definition of malicious spyware.

A malicious spyware could be one used for identity credit cards theft or which modifies file, or which gives access and control to an outsider to one's computer is undistinguishable from a malicious backdoor. There is a continuum of malicious software connecting spyware to Trojans or even "bots". The taxonomy is at the same time getting larger and more difficult with time.

3.2.4 Software vulnerability problem

Another trait of today's cybersecurity is the realization of the seriousness of the software vulnerability problem. The rate at which new vulnerabilities are discovered far from abating is accelerating. Symantec documented 1,237 new vulnerabilities between January 1 and June 30, 2004. During that period, 96 percent of the vulnerabilities were rated as moderately or highly severe. "Such statistics only underscore the fact that staying abreast of the latest protection strategies is too time-consuming for in-house staff and takes them away from other mission-critical activities".[12] It seems that basically every large software has exploitable vulnerabilities.

Against buffer overflow vulnerabilities so far there is no full proof protection. The best defense is to try to avoid creating them in the first place in the software production phase. Systems of certification for software have been developed partially to address that issue. The result has been to probably reduce the occurrence of a certain kind of vulnerabilities.

But we also discovered that there are different sorts of exploitable vulnerable, far more subtle and also exploitable but very informed cybercriminals. The number of very informed cybercriminals seems to be on the rise too. Some vulnerabilities are not detectable on the source code. They are related with the way some compilers puts the program in machine language.

The world of software security has made a lot of progress over the years. But whereas we understand better how to avoid what today looks like large mistakes (before they would have been treated as minor errors), we are discovering new scenarios of vulnerabilities and gathering evidence that we are very far from a world where software are reliable.

3.2.5 Bots

Backdoors can enter in computers in a variety of ways. It is not easy to avoid them if one does not take special precautions. A "backdoor" program gives unlimited access in a computer to outsiders. The outsider can have complete control of that computer. The infected computer has become a "bot". Networks of bots are called "Botnets".

According to a recent edition of the Symantec Internet Security Threat Report, over the first six months of 2004, the number of monitored bots rose from less than 2,000 computers to more than 30,000[13]. Botnets involving millions of computers are very conceivable and may soon appear, it they do not exist already.

Modern DDOS often use botnets. But the threat from "botnets" is not limited to large scale DDOS [14]. The owner of a botnet is in control of a very large number of computers, located in different places, belonging to a variety of users. Many bots are in fact private PC's which can belong to executives or government people or bank employees. Keyloggers can be deployed in a bot, informing the owner of the bot of everything the owner of the computer types. That can include user ID and passwords. This is used to pilfer money from banks. Bots can also be used for espionage, identity theft, getting credit card numbers. In fact there is no limit to what can be done when one controls many computers and use that control imaginatively.

Bots are relatively new. They are considered as the worst threat today, as were worms not so long ago, or buffer overflow vulnerabilities before. Today our ability to detect bots and penetrate them and identify their owners is very limited. Honeypots are basically the only tool available.

Honeypots are computers which look like legitimate computers but are designed to attract cybercriminals and document their activity. Honeypots are made into bots. This gives the opportunity to get some information on the purpose or identity of the owner.

3.3 The future

Niels Bohr has been quoted to say the predictions are always difficult, especially about the future…. The future of cybersecurity is definitely clouded with uncertainty. But given the recent trends, there is something ominous about that uncertainty.

3.3.1 Can cyberdefense move away from a purely reactive mode?

We have very limited protection today against some existing threats such as efficient flash threats, aggressive phishing, or massive DDOS, shrewd exploitation of large scale botnets, to name a few. Those are among the most visible forms of attack today that call for a much more adequate response than we have today. This is bound to be a challenge as we do not have even at the conceptual level the clear idea of how to counter those threats.

Those threats on the other hand are the threats of today. Building defenses against them is essential, but maintain cyberdefense in the reactive mode that has been its hallmark and principal weakness. We should anticipate that the pace of progress in the art of cyberattack will not abate. However astute and advanced it may look the art of cyberattack has still a lot of room for improvement. What we have seen so far may not be impressive compared to what may be in store.

Anticipating the next generation of attack on the other hand would be nice if it were even conceivable. What we can do is perceive the changes. We are transitioning from a cyberworld where a substantial number of malicious activity was done for fun more than for profit, to a new cyberworld where profit under one form of another is the goal. This means among other things passing from a world where a substantial component of cyber criminality was very visible (sometimes spectacular like some worms for example) to a new world where the cyber perpetrators prefer not to be noticed.

Many cybercrimes are made discretely. Many probably are not even detected let alone reported. Improving our detection capability of cybercrime is among the many priorities of cyberdefense. This applies not only to cybercrimes but also to their preparation, like the setting up of botnets.

Increasing that kind of cyberdefense capability is as necessary as it is problematic. It is problematic not only because it raises technical problems. Trying to make the internet less and less hospitable to any kind of malicious activity means that an increasing amount of energy and resource is put in changing the internet into a much less free place, where privacy for example may become an expendable commodity (even more than it is already the case), and will be treated as an obstacle to cybersecurity.

3.3.2 BGP vulnerability and the future of the internet

One fundamental difficulty of cybersecurity is that the users tend to be put in a situation of complexity by people who in general are more expert and inhabited by malicious intent. Education cannot do damage. But it should not be approached with the belief that it could lead to a cyberworld where the users are as knowledgeable as cyberattackers or even knowledgeable enough to be able to fend off the attackers. An internet architecture where the infra-structure itself would be less passive and more inhospitable to malicious activity would be a welcome change. In the last few years some[15] have initiated a debate to reconsider the fundamentals of the internet.

When the internet was put together, security was not a big preoccupation. Designing protocols such that different networks can speak to one another was already a significant challenge. When the internet began to grow, another challenge was to design systems of IP addresses and routing such that packets could find their ways. One challenge was scalability. The internet infrastructure, its routing system and protocol so far have been able to adjust to a rate of growth that was much larger than anything one could imagine when they were

originally designed. This is a major accomplishment. But independently of whether it is possible to do even better and add make this infrastructure even more intelligent or less hospitable to malicious activity, there is a need to address some very serious vulnerabilities of the infrastructure itself..

From a security point of view, one problem today is that some fundamental protocols like the Border gateway Protocol (BGP), which support the routing system of the internet traffic, can be abused. An efficient attack against the present routing system could incapacitate the whole internet by diverting part of or the whole traffic in "black holes", where the traffic would be lost for ever. There have been episodes in the past where by accident the internet experienced that kind of problem, at a small scale. The first occurrence may have been the notorious AS7007 incident on April 25 1997. It was caused by a router that flooded the Internet with incorrect advertisements because it had been misconfigured. It was announcing to the other routers that the Autonomous System AS7007 was the best path to most of the Internet. So a large chunk of traffic was sent to that Autonomous System (AS) and lost there as if it had fallen in a black hole. At the time this was detected rather fast. Still it took a few hours for the routing tables to be re-updated.

Different versions of the same kind of incident took place a few more times. They uncovered this realization that routers were treated as trusted systems. No authentication for a router to advertise routes. As a result the traffic of the whole internet could technically be "black holed" by a large scale attacks shrewdly designed.

Remedies for that situation have been proposed, like the introduction of an authentication system between routers (Secure BGP). Obstacles to the implementation of that kind of idea are that among other things they require a change of routers worldwide. The internet has become a gigantic infra-structure not easy to reform.

3.3.3 Potentials for really large scale cyberattacks

In addition to those scenarios of attacks, which in a sense are not new since they are subject of discussions, one has to be prepared to really new ones. The US is cyberizing its critical infrastructures, exposing them to unknown forms of cyberattacks. From the cockpit of airplanes to the manufacture of drugs, from the monitoring of patients in emergency rooms and of their treatment to the control of traffic lights in cities, the IT revolution is making its way in every aspect of the life of the US. In each case without exceptions, this will give opportunities for new forms of malicious exploitation by outsiders or insiders. Cyberterrorism, hardly a serious preoccupation today may become one soon. A massive cyberattack launched by one nation against another is not a contingency to exclude for the distant future.

The push for more exploitation of IT is irresistible in the US. It is the major driver of this cyberization. One would hope that it were possible to engineer the cyberization of critical infrastructure in such a way that it does not invite this kind of speculation. But this is not what it taking place in the US for example… The nature of cyber-exposure of the US critical infrastructure and US society in general is far too complex to permit any informed assessment of the vulnerability of the country to cyberattack today and tomorrow.

The price tag put on cyberattacks so far have been always controversial as there is no easy way to quantify those things with the scarcity of data endemic in cybersecurity. Although nobody argues that the price tag is not large and largely in the tens of billions of dollars or more. A very large scale cyberattack with a price tag to the international community in the trillions of dollars may not be farfetched in the not so distant future. What form it could take on the other hand is obviously not clear. Some have pointed out that with a large botnets having penetrated deeply in the US or international financial system, it would be possible to wreak havoc world wide at basically an unlimited scale.

The internet could be a way to jumpstart development at least this is the hope. It certainly will become a channel of communication between the South and the North. This new direct communication will take place in the destabilizing context of the huge economic inequality between the two. Already today we see the effect on the phishing and other forms of cybercriminality originating from developing countries. But the economic inequality is so large that one should not expect to see it resolved soon. What the countries of the South may not have in wealth, they do not lack in brainpower and imagination for cybercriminals of those countries. So the spread of cyberization to all nations and with it the internationalization of cybersecurity probably means not only an exacerbation of known cyberthreats, but also the creation of new ones, broadening the spectrum of cyberthreats.

4 THE INTERNATIONALIZATION OF THE DYNAMICS CYBERATTACK/CYBERDEFENSE

Cybersecurity is sometimes compared with the immune system. The immune system co-evolved with pathogens for million of years. Viruses and bacteria have become extremely sophisticated in their attack and the immune system has become very performant in its ability to detect, analyze and counter a pathogen. If cyberdefense can be assimilated to a kind of cyber immune system, this is a mixed blessing. On the one hand the notion that cyberdefense may one day be as sophisticated and performant as the immune system can provides hope for the future. On the other hand, the evolution of the immune system is littered with deaths, failures, species disappearing, etc… Furthermore the immune system is a huge organ involving 1012 cells (as many as the nervous system). In fact most of the constituents of the immune system are dual use, i.e. they have other physiological functions. If that is a metaphor for what cyberdefense may look like in the future, this means that we are very early in the process of setting up our cyberdefense capabilities.

4.1 Co-evolution between cyberdefense and cyberattack

The history of cybersecurity is the history of an arms race or co-evolution between the art of cyberattack and the art of cyberdefense. The cyberattackers have clearly the strategic advantage. They can choose their mode of attack. They have many forms of attack they can choose from. Each of them requires a different defense. Many attacks exploit vulnerabilities that are legacy of the times where security was not a serious preoccupation. Each day, sees the emergence of new exploitable vulnerabilities. Some of them are really serious. The cyberdefenders by contrast are in a permanent reactive mode, extinguishing fires, trying to fill holes and ensure that the same attacks do not do the same damage again. Each new cyberdefense system seems to inspire cyberattacker a new way to circumvent it… This somewhat chaotic dynamics of co-evolution has yielded the no less chaotic system of cyberdefense that exists today. However chaotic it may be, it seems to be doing a reasonable job at maintaining the cyberthreat at an acceptable level.

The internationalization of cybersecurity through the addition of developing countries exacerbates some pre-existing problems and adds new ones. Among the unanswered questions is whether the present self-organized structure of defense will be adequate to address a threat in some sense qualitatively different. In the present “system” of defense in advanced cyberized country, the private sector represents an important bastion for cyberdefense. Key aspects of our cyberprotection (like anti-virus defense) are completely done by the private sector (in that case Symantec and its competitors). In the US, in principle the private sector and public sector collaborate. In practice the private sector tries to keep the government and law enforcement at a safe distance and has been working (so far successfully) at limiting regulation and legislation dealing with cybersecurity. Instead individual private companies acting individually or in some form of cooperation or private consortium and little help from governments have developed a defense system adequate to their needs so far. If and when it may have to deal with more formidable cyberthreats, the private sector may change its attitude.

It is noteworthy that when it comes to international monitoring capability and world wide realtime traffic analysis, nobody comes close to Symantec. Through contracts with customers, Symantec has permanent access to 20,000 sensors distributed into about 180 countries.[16] It has impressive control rooms in the US (Alexandria, Va), UK, Germany and Australia, where operators analyzes 24/7 in real time the internet traffic world wide. No government agency or group of government agencies has capability which even remotely compare.

This puts Symantec, a private company, in a unique position of influence and responsibility. Cybersecurity has ushered the US in an era where cooperation between government and private sector is central to the posture of the country. In the field of security, what Symantec can do for the governments is clearer than what governments can do for the company. Symantec is not the only private company with huge clout in cybersecurity. Verisign would be another example. So far this reliance on the private sectors has probably proved successful, in the sense that it has contributed to the flexibility and efficiency of the response. The unsettling aspect of that set-up is a private company works for profit and it does not need to operate at the same level of accountability as a government.

The co-evolution cyberdefense cyberattack is far from over. As cyberthreats change, so will companies like Symantec. Presumably they will continue to address that part of the changing threat they think appropriate or for which they have a comparative advantage, leaving others address the other threats.

4.2 Internationalization of the problem

Cybercrimes can be committed basically in any country from any country. The fact that cybercriminals often reside in foreign countries create all sorts of complications for the law enforcers and those charged with the investigation. Hotbeds for different forms of cybercriminality appear and shift with the waves of cyberization and as a result of the international response. Russia and eastern Europe just after the fall of the Soviet empires were among the first countries to produce cunning hackers able to cause mayhem. Before that the Balkans seemed to be a hotbed for malicious codes. Otherwise most of the cybercriminals were located in the US and to a lesser extent Western Europe. Being a hacker was not necessarily a form of cybercriminality. A distinction was being made between hackers, crackers, script-kiddies, between the developers of tools and their users, between Black Hats and White Hats.

Most of those distinctions point to an era where cybersecurity was far more benign than is the case today. The internationalization of cybersecurity is not new. Some well-known worms (like the I love you virus) originated in foreign countries. The attempt of extortion referred as 419 and attributed to the Nigerians originally has been around for years.

We are witnessing an accelerating internationalization of cybersecurity, where the targets tend to be in rich countries and the attackers distributed in the whole world.

4.2.1 The geographic distribution of hackers and cybercriminals is not uniform

It is difficult to have a very precise picture of the international situations because of the scarcity of reliable data. Most of the available data are based on accumulation of anecdotal information…

Keeping this caveat in mind, according to the Texas based ClearCommerce[17] and a Verisign report[18] , the ten countries leading in cyberfrauds by volume in 2004 were: US, Canada, Indonesia, Israel, UK, India, Turkey, Nigeria, Germany and Malaysia. The US tops all the lists “by volume” of cybercrimes of any kind because it is the country with the highest and most diversified cyberactivity.

Probably more interesting for this discussion is the list of the ten leading countries in cyberfrauds by percentage of transactions. In 2004, they were: Indonesia, Nigeria, Pakistan, Ghana, Israel, Egypt, Turkey, Lebanon, Bulgaria and India. By comparison, in 2003 Indonesia was second behind Ukraine. Somehow Ukraine seems to have lost of its luster, whereas Paraguay has been mentioned as a new entrant with “serious” potentials.

When it comes to hackers the situation is more complicated. The numbers of hackers is only one piece of information. Another is the kind of hacking they do. Brazil[19] is one of the leaders in hacking[20] . But the Brazilian hackers tend to be less sophisticated than their rivals or colleagues from Russia. They look like script kiddies compared with the more sophisticated Russian hackers.

The Russian police boasts that the Russians are the best hackers in the world[21] : "Everyone knows that Russians are good at maths," said Lieutenant General Boris Miroshnikov of the division known as Department K. "Our software writers are the best in the world, that's why our hackers are the best in the world."[22]

Another reason may be that the social context is different. In Russia, hacking and cracking is pursued aggressively by organized groups. In fact we do not know exactly the extent of their exploits.

Hacking in Brazil is apparently facilitated by the fact that the cyberlaws are allegedly lax[23] . Many hackers are closer in style to the teen age script kiddies who were so common in the US and Europe not so long ago and who exposed unbelievable holes in the cyberprotection of military secrets in the US Departement of Defense. This is still happening.

The Global Command Centers[24] (a company which “monitors and protects client networks from cyber-attacks”) puts Malaysia among the top three countries for intrusion attacks. According to e-Cop.net the top five countries for intrusion attacks were the United States, Russia, Malaysia, Singapore and Australia.

Depending on the source the lists out leading countries vary somewhat. But it is a fact that today the geographic distribution of cybercriminality is not uniform. But it is not static either. What are the forces of change and what cyberworld do they lead to?

4.2.2 Spam, Phishing and identity theft

Spam and phishing are probably the forms of cyberattacks that the average netizen experiences the most directly. Both have a strong international dimension, in different ways.

4.2.2.1 Unchecked, spam has the potential to affect the economy of the internet

According to SpamHaus[25] , the ten worst spammers today are: US, China, Russia, Japan, Canada, Taiwan, South Korea, Netherlands, UK, Hong Kong.

In that case, the US is at the same time the worst culprit and the biggest victim. By contrast, China (the second spammer country) is basically a beneficiary. China sold a lot of URLs used as spam servers (the number 1.7 Million circulates). The spam emanating from those servers is sent to the rest of the world. It is not intended for the Chinese people, but it brings money to the Chinese who sell the URLs.

This is one reason why an important date in the anti-spam campaign was when China accepted to sign the anti-spam pact in July 2005. The pact, launched in September 2004 is the result of a anti-spam campaign led by the UK and US. About 30 countries have joined the antispam pact so far. Through a world wide campaign of workshops and conferences the governments of developing countries are being alerted to the problem raised by spam. The pact has entered into force in China in early 2006. So it is too early to see whether this made a difference.

International cooperation is crucial for the future of cybersecurity. There is a considerable uncertainty as to how committed the different governments will be. The degree of success of the anti-spam pact (measured by the evolution of the membership of the anti-spam pact and of the amount of spam circulating with the mail) will be monitored closely as it will represent interesting indicators for the future of international cooperation in cybersecurity.

The approach through an intergovernmental anti-spam pact is not the only avenue to combat spam. In addition to personal filters, ISP's for example, could also play an important role in filtering large chunks of it. In fact already most ISPs refuse to carry spam knowingly. For an ISP to take that traffic for profit is called "going pink".

Spam has been one instance where governments have played a role. Costa Rica provided an example of that. Costa Rica was once a leading "spammer" country, to the extent that ISP's began to refuse to carry traffic coming from that country. As a result, the government of Costa Rica intervened to re-establish the cyber-respectability of that country and its connection to the rest of the world.

From a technical point of view, spam presents a lesser challenge than other cyberthreats. If the antispam pact turns into a success, this would be a promising precedent. If its record turns out to be mixed or even mediocre, this will be interesting also as it will inform us on the difficulty of countering cyberthreats.

The anti-spam pact is one instance is an intergovernmental agreement. This is in a context where the US government has a limited role in the governance of the internet in the US as well cybersecurity. The scenario whereby solutions to cybersecurity problems are found in international agreements between governments is bound to change this situation. It will confer a growing role to governments in the governance of the internet. However unavoidable it may be, this evolution is not without problems. On the other hand, considering the kind of challenges that cybersecurity represents for the international community, close cooperation between all the governments is of essence.

4.2.2.2 Identity theft and phishing

Identity theft and phishing have been around for some time and are far from abating[26] . Phishing has for a long time had an international dimension. Phishing is based on an interaction between the victim and the attacker. Up until recently English was the lingua franca of Phishing. This is changing… Identity theft is rampant. Law enforcement is an important component of the response. When the criminal lives in a country far away, he or she may feel the threat from law enforcers.

4.2.2.2.1.1 Phishing

The Nigerians (under the name 419) are credited for the invention of a form of phishing which exploits the gullibility/greed of netizens by promising them a large fraction of a large sum of money difficult transfer from that country. After all these years, this era is not over. Apparently hundreds of Millions of Dollars are still pilfered that way, yearly. The fact that so many still fall for that trick is an indication of how serious the threat of phishing is for our society. Today there are far more sophisticated forms of phishing being used, which works against well-informed netizens not easily abused. In fact phishing can be so sophisticated, that it can be positively difficult to realize that one is a victim of it. Paranoia may be the best or only protection… In March 2006 for example, hackers (who turn out to be based in Korea and Poland) managed to induce French citizens to reveal details of their banking account by posing as officials from their own banks (Société Générale, Crédit Lyonnais and BNP Paribas), explaining to them in convincing terms that they had to re-enter their coordinates for verification. The websites of the banks were perfectly reconstituted and the whole story was presented in such a way that it looks perfectly plausible[27] .

This kind of stories is unfortunately not uncommon. What is noteworthy is that it illustrates the internationalization of the targeting. The victims of Phishing are not anymore almost exclusively English speakers. Now they can speak other languages[28] . This broadens the "target pool".

4.2.2.2.1.2 Identity theft

Exploitation of Identity theft has been a problem for years and this is an area where the cyberdefense has not improve significantly. There are reasons to believe that there are far more cases of identity thefts than those reported. Furthermore the number of success stories for the defense is small. And the success stories tend to be the same ones, like for example the famous classroom example of the "Russian hacker", which comes back now more than 5 years. That case is also interesting, because although it is presented as a success for law enforcement, it also reveals limits of our response capability, which o a large extent are still there.

4.2.2.2.1.3 Russian hackers

In 1999-2000, hackers "would post non-existent products to sell on e-Bay. Different scripts would pay with stolen credit cards, which would cause payments to precipitate into PayPal accounts that another script created. Then a different set of scripts would create and generate email acknowledgements to the "buyer" and "seller," simulating the e-Bay process. By keeping credit card transactions below a threshold, they avoided triggering undue scrutiny. In less than 9 months, credit card companies were defrauded of over $25 million dollars" [29].

Some banks reported anomalies to the FBI and eventually an ISP in Seattle complained of an attempt of extortion that was accompanied by significant cyberattacks. The FBI investigation established that this was coming from what transpired to be two young hackers based in Chelyabinsk, in central Russia. One oddity in this case is that the two hackers were apparently interested in jobs in the US and apparently thinking that they could get away with what they did to the ISP in particular. The FBI built a fake company and invited the hackers to come for a job interview. The hackers accepted the invitation to be arrested by the FBI. The two Russian hackers were eventually sentenced to a few years in US jail each.

This case has been analyzed in great details and points to several still unsolved problems. It took 417 hours of investigation plus two years in court (with conviction of a few years for both defendants) to sort this case out[30] . How to improve the cost efficiency of the response is unclear. The post mortem analysis revealed that there had been "system security failures and business process trust collapses [which are] attributable to inappropriate application of technologies/products [and] lack of appropriate security engineering process during system development phase"[31]. In other words what these Russians wanted to do could have been detected earlier and a lot avoided had everything worked perfectly. A lot of recommendations can be made regarding what can be done to enhance security and trust requirements at the levels of business transactions and processes. But these recommendations aim at avoiding the repetition of previous mistakes, not to prepare for the next one. In this case human errors were involved.

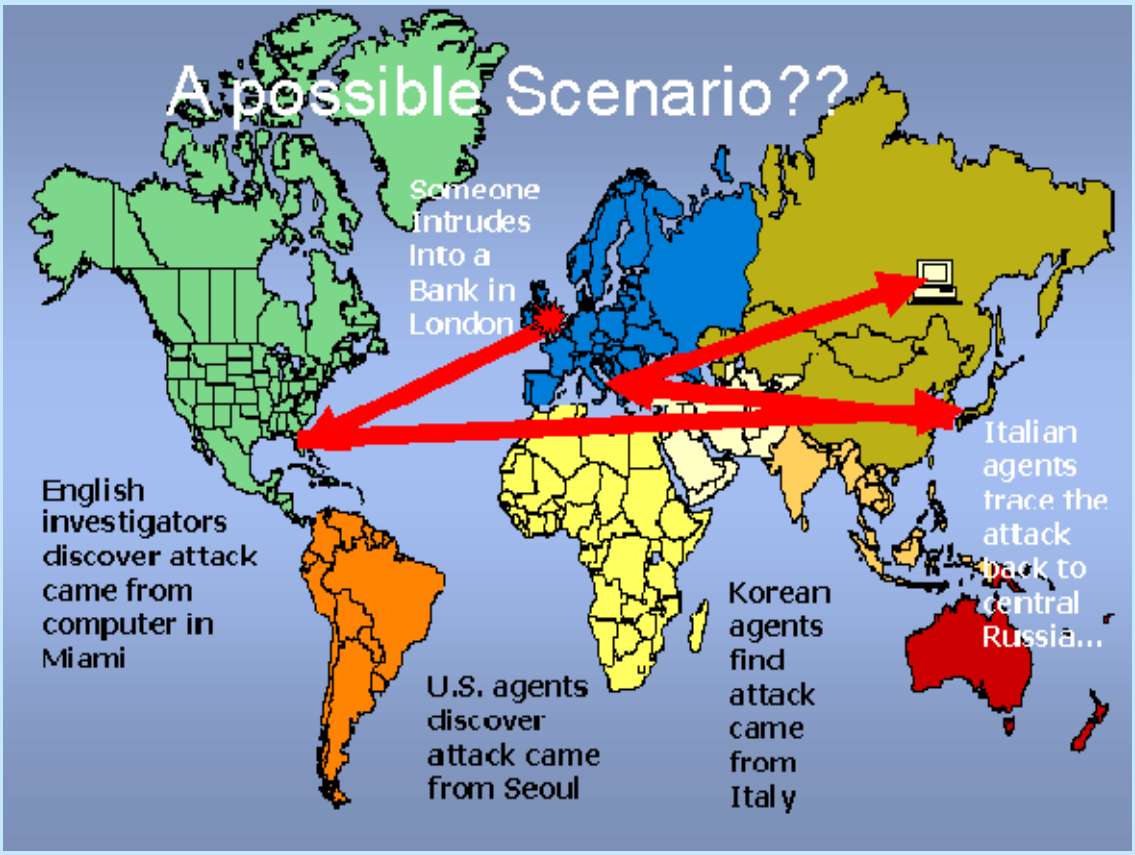
An utopian world where no mistakes are ever committed and no system failures ever occur, would be much more robust against cyberattacks than a world made of human beings prone to mistakes, where computer

security is so complicated. The kind of glitches that made the exploits of the two Russians possible are not shocking or uncommon. This incident took place in 1999-2000. But similar mistakes are most probably being made today. Using the same kind of techniques as the original "Russian hackers" or improved versions of them, it is not difficult to imagine what better organized hackers would be able accomplished or are accomplishing as we speak… The Russians do not have the monopoly of identity theft or other form of hacking from abroad and the number of recorded cases of identity theft is apparently increasing.

4.2.2.2.1.4 Tracing back the origin of attacks and the 24/7 network

One difficulty is to trace back the origin of a cybercrime. Attacks are often designed to be difficult to trace back. With the present system of internet protocol it is not so easy to make the reconstitution of the trail. This requires the help of several players located anywhere in the planet, who have access to logs of the traffic. This pre-supposes that a record of the traffic is kept and that one has the data mining capability to search it. Depending on the situation both of those conditions can be problematic.

Figure 1: Hypothetical Traceback scenario

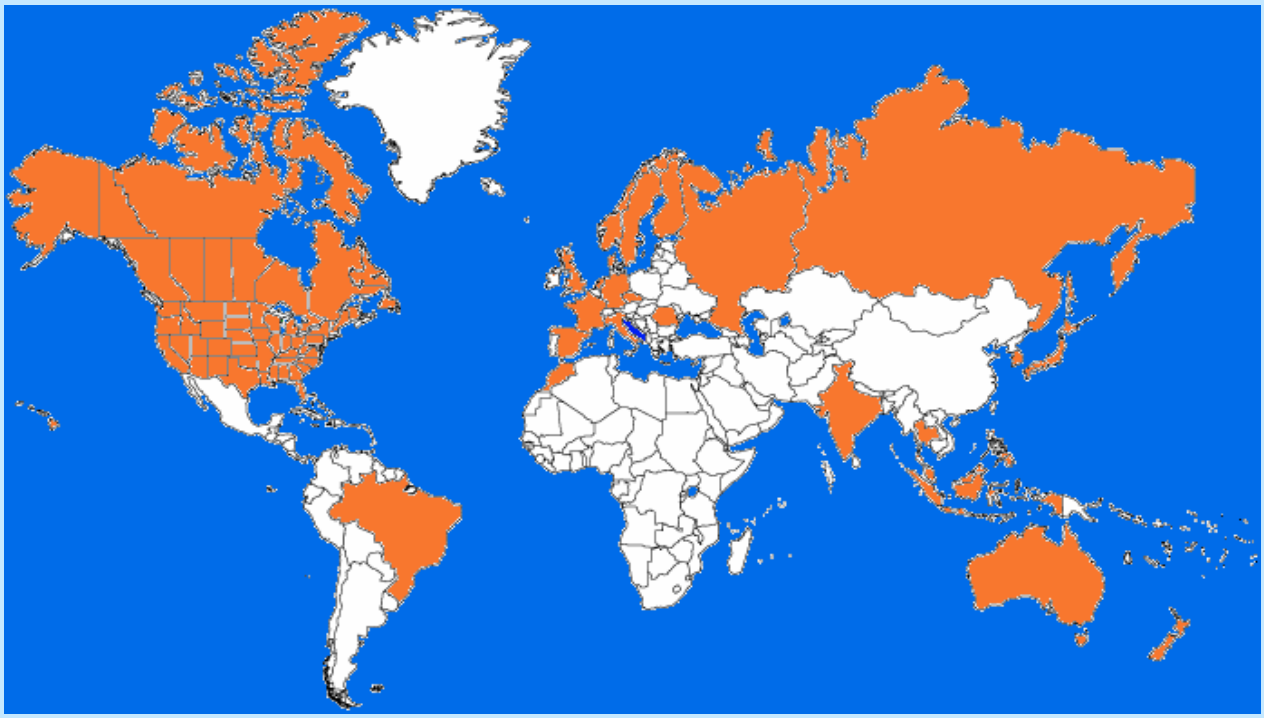


This supposes also that there is agreement across nations to share that information in a timely way. This is the goal of the so-called 24/7 network, which has been created after a meeting of the G8 Justice and Interior Ministers meeting in Milan in February 2001. The goal is to "facilitate and expedite the tracing back of cybercriminals". Members of that network are supposed to provide a Point of Contact (accessible 24/7) and help investigations.

The agreement comes under the form of recommendations to Governments like taking "steps to be able to trace more effectively international terrorist and criminal communications. The Recommendations address a broad range of issues, including preservation of data relating to specific investigations, expedited legal assistance, real-time tracing through multiple providers, and user-level authentication." It is specified that there is requirement to enhance existing technical capabilities….

The membership of the 24/7 network as of 2003 is shown in Figure 2[32].

Figure 2: Membership of the 24/7 network in May 2003



Source: http://www.apectelwg.org/e-securityTG/clecb/DOWNING.ppt

This map is interesting for its membership. Brazil is the only Latin American country and Morocco the only African country. Those two countries happen to be leaders in their respective continent in internet penetration.

In Europe, Rumania is the first Eastern European country to join. Ireland, Portugal, Switzerland, Austria and Belgium, decided not to join immediately the network.

In Asia, Russia, India, Thailand, Malaysia, Indonesia, South Korea and Japan were the only countries, which join early.

The 27/4 network paradigm works only if eventually all nations join. Otherwise this creates havens where hackers can hide their trail. On the other hand keeping record of all the internet traffic raises issues of privacy. Who should be the guardian of that information? In most countries like the US, this information has to be retained by private ISPs. How long should it be kept? Who should be allowed to access that information? Under what condition?

Nations approach these questions differently. These differences reflect the complexity due to the diversity of situations. This diversity reappears in many other aspects of cybersecurity and is a complicating factor in the implementation of a regime which requires so much international cooperation.

4.2.3 Infections

In the same way that the number of infections can inform on the health level of a country, computer infections inform about the cyber-health of countries… A distinction has to be made between different forms of infections. Here we distinguish between infection by zombies, spyware and viruses.

Zombies are a certain kind of backdoor programs. They entered a computer in general thanks to a worm and after installing themselves are dormant in the computer up until they receive a signal, or simply a specific date. In general they are programmed to wake up at the same time as a large number of other zombies. All

these zombies make the computer they infect make queries to some targeted website in such a way that the site gets saturated and unable to respond. In other words, zombies participate to Distributed Denial of Service attacks (DDOS). Infection by zombies is an indicator the number of computers that have been successfully infected as prelude to DDOS.

Spyware are programs which record the internet activity of a user for the benefit of a third party. One possible goal can be to profile the user for commercial purpose. But since the user is unaware of the presence of the spyware, the goal could be far more malicious.

Every day new computer viruses are released. They tend to propagate as e-mail attachment. The distinction between virus and worm is a subject of debate. A popular distinction is to say that a virus requires the action of a human being (like opening an attachment) to spread whereas a worm spreads by itself. Others try to base the difference on how viruses infect files and/or program to multiply. Many implicitly or explicitly behave as if the distinction is not very clear or useful and use both terms indifferently. Antivirus software are sensitive to worms and viruses equally. They can detect other malicious codes such as Trojans or backdoors. The level of virus infection informs on how widely antivirus software is distributed and how regularly and fast it is updated.

In advanced cyberized countries, there are incentives to update regularly antivirus software. Since new viruses are detected basically every day, it takes a very regular updating to limit their spread. Virus infection may cause damage to the files or hard disk of the computer. Disinfection can be time consuming, costly and disruptive.

In developing countries the additional consideration is the cost of antivirus software. It is a much more serious consideration than in richer countries. This makes virus management more difficult and explains why virus infections tend to be more problematic in poor countries.

4.2.3.1 Infection by zombies

Zombies are the programs used in DDOS. Infections by zombies are connected with the threat of DDOS, in the sense that infected computers are the ones used in the attack. According to prolexic, the ten countries most infected by number of zombie infections are[33] : US, China, Germany, UK, France, Brazil, Japan, Philippines, Russia, Malaysia.

The top ten countries by number of infections per capita are: Hong Kong, Germany, Malaysia, Hungary, UK, France Taiwan, Australia, US, Spain.

The interpretation of those data is not completely obvious. If one limits the comparison to US, UK, Germany and France. The comparison suggests a similarity of situation between these countries. In each of them there is a large and comparable DDOS activity going on. DDOS is a problem for e-businesses. So far it seems to be a problem for advanced cyberized countries.

The presence in these lists of countries like Malaysia for example is more problematic. It has the reputation to be active in cybercrime, but inside the country there are not so many targets for DDOS. Targeting a website from another country does not seem very efficient, because the malicious traffic will have to go through bottlenecks on its way to its victim. This makes filtering of that traffic close to the source much easier than in the case of a modern DDOS using botnets.

4.2.3.2 Virus infections

Viruses are produced world wide and spread everywhere. No country has the monopoly. Some achieved visibility at some points. Bulgaria for example has been called a “virus factory”. The virus “I love you”, which made it to the first page of the newspaper in 2002, was the work of a young drop out from college in the Philippines. Code Red a worm which made headlines in July 2003, is strongly suspected to be originally Chinese.

The virus SoBig (released in Summer 2003) came in different variants. Its sixth variant (SoBig.F) was so successful that Microsoft together with Interpol and FBI set up a system of reward ($250,000) for information leading to the author(s). On the basis of forensic analysis and comparison with other viruses, it has been suggested that the SoBig viruses were written by a well known Russian group: the team of the

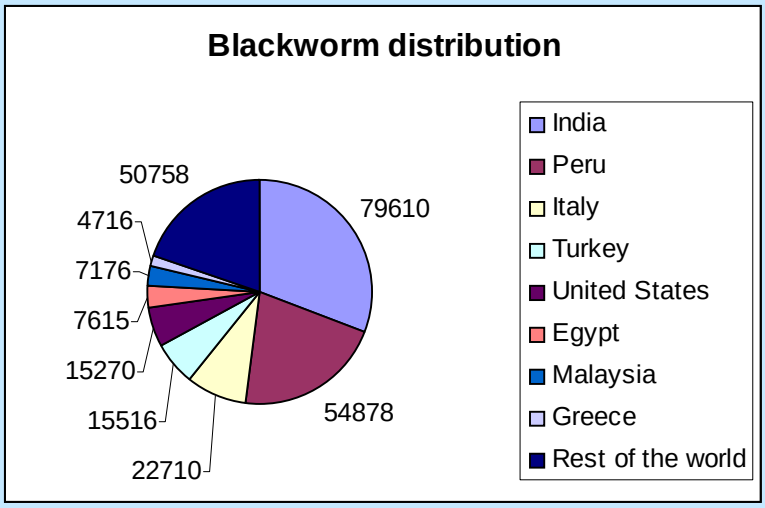
famous Rusland Ibragmov, based in Moscow[34]. Ibragmov denies vehemently any involvement in the making of that particular virus.

Many viruses are variations on previous ones. As a result viruses sometimes come in dynasties (SoBig for example, had at least 6 versions: SoBig.A, SoBig.B, SoBig.C, SoBig.D, SoBig.E and the famous SoBig.F. The well known Blaster had at least 8 versions, MyDoom had in excess of 30 different versions, Beagle had in excess of 60 different versions. [35]).

Every day Symantec or McAfee reports new viruses. The number of viruses and worms which have been released over the years is in the thousands. For some reasons, most viruses are not very successful, but when they are, they can make the first page of the newspapers. What determines the degree of success of a virus is the speed of its propagation compared to the speed at which its existence is detected, rate at which infected computers are withdrawn and disinfected, the time it takes to find a signature to be added to antivirus software and the speed at vulnerable computers are made immune by updating the antivirus software. In rich countries this takes place more and more efficiently thanks to Symantec and its competitors. But those are commercial companies. If a poor country could not afford this kind of response, it would be far more affected by the same virus.

The virus Kama Sutra (Released in March 2006, it was also called Blackworm, Mywife, Nyxem, Blackmal or Grew) is interesting for the geographical distribution of its infection[36].

Figure 3: Geographic distribution of the worm Kama-Sutra



Note: The numbers come from LURHQ, http://www.lurhq.com/blackworm-stats.htm

Compared to the rest of the world, Peru and India were disproportionately affected by the virus Kama-Sutra or Blackworm. There is no definitive explanation for that. The way the virus was seeded initially may have to do with that. This chart shows only the recorded infections. There is the possibility that many infected computers were not recorded. In Vietnam for example a survey of 2,000 users by the Hanoi University of Technology's Bach Khoa Inter-network Security Center (BKIS) showed that 94 percent of the computers in the university to be infected with viruses, and 87 percent with spyware and adware.

The reason why India or Peru seemed to have been more affected could be related to the fact that anti-virus management is less efficient in poorer countries. If one computes the number of infections per internet user, Peru would be the most affected (1.5%), before Malaysia (0.2%), a group made of India, Egypt, Turkey and Greece (~0.15%). Italy and the US by comparison were much less affected.

One thing is sure is that in Peru and India among others tens of thousands of computers had to be disinfected. For a developing country the cost of disinfecting such a large number of computers is serious. For developing nations, virus management can be an expensive proposition. In many cases, the level of antivirus protection is lacking and disinfection is far from automatic. As a result, in our globally connected world viruses and worms linger much longer if not forever.

In that context China and its quixotic approach to intellectual property offers an intriguing example. In that country pirated anti-virus software can be downloaded for free from hacking website. However abhorrent this notion can be to defenders of intellectual property rights, from the perspective of international antivirus protection and containment of virus infection, there are some advantages in the Chinese approach… Antivirus software is the purview of private companies. They do that for profit, like pharmaceutical companies sell drugs for profit. Pharmaceutical companies make exceptions sometimes for developing countries… It is difficult to believe that the same will happen with antivirus software.

Virus management is part of a larger issue looming at the horizon of the internationalization of cybersecurity: the economics of cybersecurity.

Cybersecurity comes at a cost. For the same reasons that PC's are too expensive for netizens of many developing nations, minimal protection measures like antivirus software for many of them looks like a kind of luxury. And antivirus software is by no mean the only costly item in cybersecurity.

5 GLOBAL CYBERIZATION AND THE CHANGING CYBER-SECURITY WORLD MAP

After its spectacular growth in rich countries, the internet is spreading to the rest of the world. Even if the internet is already considered an international critical infra-structure connecting the whole planet, in fact the penetration of the internet in most of the world is only beginning. The cyberization of the developing countries is probably the most important factor of change in cybersecurity. If the cyberattacks of the future may dwarf what has been experienced so far, it is not only because the cyberattackers are getting better, it is also because their number and their playing field is increasing.

5.1 Multi facets of cyberization

5.1.1 Cyberization is global

In every country the internet seems to have an irresistible appeal. In developing countries where computers tend to be expensive, internet cafés are omnipresent. Their number is increasing even when the internet connection is limited. In most developing countries the internet plays at best a limited role in the economy. But progressively its role is growing, sometimes by design, but also because as a result of a natural push.

The process of cyberization is global. The number of people connected to the internet has been increasing fast in the last five years, everywhere (Cf Table 1), everywhere in the world. But the degree of internet penetration is far from uniform. However fast the growth of the internet seems to be, it is obvious that it will continue to grow for a long time in the future.

Table 1: Internet Penetration worldwide by continents

World Regions	Population (2006 Est.)	Internet Usage, Latest Data	% Population Penetration
Africa	915,210,928	22,737,500	2.50%
Asia	3,667,774,066	364,270,713	9.90%
Europe	807,289,020	290,121,957	35.90%
Middle East	190,084,161	18,203,500	9.60%
North America	331,473,276	225,801,428	68.10%
Latin America/Caribbean	553,908,632	79,033,597	14.30%
Oceania / Australia	33,956,977	17,690,762	52.90%
WORLD TOTAL	6,499,697,060	1,018,057,389	15.70%

Source: http://www.internetworldstats.com

5.1.2 The cyberization of developing countries brings new hackers

The spread of cyberization to developing countries brings new scenarios of cyberattacks and new hackers. In developing countries, the hackers are among the first to be interested in the internet and they are among their most intense users. Although there are no reliable numbers to back this assertion, it is safe to assume that in developing countries with low internet penetration the proportion of netizens who become hackers is much larger than the average in richer societies. Indirect evidence of that is illustrated by the fact that the countries where the number of cyber-frauds as a proportion of cyber-transactions is the largest, are countries like: Indonesia, Nigeria, Pakistan and Ghana. In those countries where e-banking and e-commerce are poorly developed if they exist at all, the access to the internet means (among other things) ability to engage in international cyber-fraudulent activities.

As a result the world of hacking is changing. New styles and techniques are appearing. They also tend to be the most knowledgeable users of the internet in those countries, far more knowledgeable often than the representatives of the national authority (when it exists) in charge of cybersecurity. Not only do they tend to be the best experts in cybersecurity in those countries, but they also learn and improve fast. We have not yet seen the full impact of this phenomenon.

5.2 The forces of cyberization in developing countries

Some developing countries have ambitious ICT plans and the push for the cyberization comes from the government. The active promotion of ICT is official policy in many developing countries like to name a few: Thailand, Vietnam, Rwanda, Cambodia or Egypt. From an economic development point of view those policies (when they are pursued seriously) are extremely interesting experiments, which may help us understand better the interaction between information technology and economic development. Little is known on this subject except that they are clearly coupled.

In many cases the commitment of the government seems ambiguous. In Cambodia or Egypt among others, the internet is perceived by the government as a disruptive technology. It puts constraints on what can be done and bans access to selected websites.

In countries like Cuba access to the internet is very restricted. China is notorious for its “great firewall” and intolerance of expression of political dissent through the internet.

Even when the use of the internet is not encouraged, the desire to be connected to it is so intense and universal that the push for its growth overwhelms the ability of government to stop its growth. In other words, that form of cyberization - access to the internet - does not need the prodding of governments. It is a global and irresistible phenomenon. Computers exceed the budget of most of the citizens of the developing world. Cybercafés provide a more affordable access. In developing countries the intense demand for internet access, worldwide is reflected in the fast spread of internet cafés.

The new breeds of hackers joining the internet are often based in cybercafés, which sometimes (the warnets in Indonesia for example) can become hotbeds for cybercriminality. The fact that developing nations shelter hackers puts their government under some pressure to do something about it. They sometimes do…

In today’s world, basically no developing nation is immune from the process of cyberization. But few if any take its companion, cybersecurity very seriously.

Enough has been learned about the e-economy over the years in the more cyberized countries to know that cybersecurity is not to be neglected. One clear message of the short but turbulent history of cybersecurity is that the internet allows all sorts of malicious activity which have the potential to erase its economic benefit.

For developing countries the problem is compounded. They are less robust financially than the rich countries. A campaign of virus disinfection can easily cost in excess of tens of Millions of dollars. What is affordable for some countries may not be for others.

Another consideration is that in cybersecurity there is a learning curve. Books do not substitute for experience. Managing security can translate into many different things. The level of cyber savvy of the experienced cyberized society is the result of many years of experience. A lot was learned the “hard way”. And still today cyberattacks can do a lot of damage. Developing countries will have to go through a transition between a pre-cyberized state to a situation where assets will be accessible from the internet. This

will be a very dangerous transition in today's aggressive security environment, for countries which can ill afford significant losses.

It is unsettling therefore to see that in most countries engaged in cyberization, cybersecurity is not taken seriously. In fact the problem is already visible in the World Bank, which funds ambitious ICT projects with cyber components and which does not seem to think that cybersecurity is important enough to justify a separate budget and a detailed plan. This takes in a world where two major international institutions - the UN and the OECD - both preached the need for spreading of a "global culture of cybersecurity". Their recommendation can be heard over and over again in every relevant forum. But it is not an exaggeration to say that those have been so far empty words. Do those who speak of "culture of cybersecurity" know what they are speaking about?

As a result the cyberization of the developing countries is best described as backing into what may turn into a series of troubles.

5.3 The contrasts in the cultures of cybersecurity

The concept of "culture of cybersecurity" deserves attention. It was used in the UN resolution and was introduced in the OECD "Guidelines for the Security of Information Systems and Networks", published in 2002.

In those guidelines, OECD defines "culture of security" as "a focus on security in the development of information systems and networks and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks".

In practice, the term culture of (cyber-) security does not mean the same thing for everybody, except maybe for the "focus" on security.

Policymakers and "practitioners" do not have exactly the same perspective on this subject. The policy makers may already differ among themselves. Some policy makers may put the emphasis on the law enforcement/cybercriminality aspect of cybersecurity, while others will be more concerns with the impact on the economy or others still on the national security dimension. All translates into some form of culture of security, but with different emphasis.

For most "practitioners", a culture of cybersecurity refers to cybersecurity savvy and expertise like how to make networks robust to cyberattacks or ensure the security of data (i.e. their integrity, availability and confidentiality). There is an overlap between these different conceptions, but that should not conceal the fact that there are also important differences.

When it comes to developing countries the perspective of policy makers is essential as they are the ones who are responsible for introducing that culture. When it comes to cybersecurity, the instinct in developing countries seems to be to build national CERTs (Computer Emergency Response Teams) or CSIRTs (Computer Security Incident Response Teams).

This is probably not a bad idea. But the premise is that the American CERT represents a useful precedent that has to be emulated. That is more questionable. The cybersecurity situation in the US is as complicated as it gets and the role of CERT in the US is very different from the paradigm that could be useful in developing countries. That paradigm has still to be invented and to a certain extent should be different for each country. Still the know-how needed to build such national institutions is best found in the US. But it is somewhat scattered in many places.

6 THE CHAOTIC WORLD OF NATIONAL CYBERSECURITY SYSTEMS

6.1 The US example

In a cyberized society, cybersecurity is at the vortex of concerns with e-commerce and the economy as a whole, e-governance and the functioning of the government in general, the protection of critical infra-

structure and national security, criminality and law enforcement, among others. One would expect that cybersecurity would be treated by governments of countries in an advanced state of cyberization, as an important priority. This is not what happened in the US, at least not yet.

In fact the political and Congressional debates in the US on this subject are anything but informed and mature. There seems to be no agreement on how seriously the government should be involved in cybersecurity. The agency in charge of cybersecurity in the US government is called the “National Cyber Security Division (NCSD)”. It was created in June 2003 as a subdivision of the Information Analysis and Infrastructure Protection (IAIP) Directorate, itself located inside the Department of Homeland Security. The most common criticism against that set-up is that it buries the responsibility for the security in cyberspace at a relatively low level in the bureaucracy. One effect of giving so little clout to this agency, is that it is very limited in what it can do. In the spring 2004, Senator Lieberman (D-Ct) for example asked angrily: “why is it that all the administration had to show at a National Cyber Security Summit last December (a summit organized by NCSD) "was neither a plan nor a blueprint, but a plan to create a blueprint?". It has been difficult to find a head for NCSD. Well known people like the previous “cybersecurity Czar” of the White House refused the jobs. The first one who accepted the job resigned in frustration eventually…

It is fair to say that the US does not have a well coordinated government cyberpolicy. But at the same time the US is a leader in cybersecurity. Up until recently cybersecurity concerns grew and evolved with the growth of the internet. CERT (created in 1988) played a central role. Its role was not to champion a US government policy. It has been through its advisories and statistics to disseminate an information, which played a key role in the level of awareness worldwide. A whole cybersecurity culture emanated from there on which the cyberdefense is based in the US and in the rest of the world. The government plays hardly any role today is the cyberprotection of private companies. In fact they have been fighting as far as they could regulations and legislation on this subject. Still some new laws like Sarbannes and Oaxley (in reaction to the Enron scandal) forced them to meet higher integrity standards in data management, at a significant cost. But when it comes to build responses and protection against malicious attack, the private sector in the US, acts on its own. There are quite a few consortia they have build, they can hire the service of a variety of for profit firms, large organizations have their own CERTs, many of which are among the 178 members of the Forum of Incident Response Teams (FIRST). National CERTs account for only about 17 of them, i.e. about 10%. Private organizations such as the SANS institute (there are many others) appeared spontaneously, with as goal to educate and inform about this complicated and confusing subject. The SANS (System administration Audit Network Security) institute is a cooperative research and education organization created in 1989 well known for the quality of its contributions like papers and security alerts. Some giant companies like Symantec also established themselves as the main providers of software protecting potentially the whole world against the new malicious codes being released every day. Important parts of our cybersecurity depend on them.

In other words, the present cybersecurity system in the US is not the result of a plan. It self-organized itself around perceived need with the adaptivity of a free market system. The result is a chaotic system, which so far does the job. But it is not a reproducible paradigm.

Following the same path is not advisable for countries undergoing cyberization now. Had the cyberthreat been as formidable back in the early time of the internet as it is today, it is not obvious that the internet would have been perceived as much a source of business opportunities to the extent it did. What is obvious that if the government wanted then to see the internet offer that kind of opportunity, it would have had then to take its responsibility as government with respect to cybersecurity much more seriously.

For the same reasons, nations starting now to try and reap the benefits of an information-based society, e-commerce, e-governance, e-education, e-health, in today’s world, will not get much of those benefits if they are not aware of what today’s cyberthreat is and how to avoid to suffer its full effect. That calls clearly for some form of national cybersecurity policy and an agency to implement it.

If the US cannot be used as a template, what should? In fact there is no country so far that can be pointed to as a good template. Countries of Western Europe, for example are in a situation not dissimilar for the US. They develop their own capabilities along the ways. There are CERTs all over Europe, some belonging to firms, some associated with parts of the government such as some ministries. There is no perceptible difference in cyber-savvy between Europe and the US. But Europe has not much to offer to the rest of the

world, with the noteworthy exception of the cybercrime convention. However imperfect it may be (it drew a lot of criticism), it is the best hope of a convention on that subject which could be the foundation of an international system to deal with cybercrime.

6.2 Lessons for developing countries

If the US and Europe do not have much to teach to developing countries with their institutions, they have a lot to contribute to the knowledge. So has Australia, which in fact is credited to be among the most active countries in disseminating the right kind of knowledge to developing countries.

Whereas there is no doubt that all governments in developing countries should have or acquire a cybersecurity capability, one should be too prescriptive as to the exact form that such capability should take. Not enough is known about the subject and the specifics of every nation to justify a one-size-fits-all approach.

A few conditions have to be met for such an agency to perform. The most obvious one is the technical expertise. Computer science is a complicated world. Cybersecurity exploits aspects of it which are not easy to grasp. New "exploits" are often very shrewd and their mechanism not so easy to understand. Security experts scattered in different institutions private or public are often the first to understand and the people to turn to have a proper explanation. Their explanation is in general a simplification. Clearly a high level of technical expertise is needed in each of these agencies. Considering that cybersecurity evolves fast, that technical expertise has to be maintained. Governments of developing countries should have a place where they can send their technical experts. As of today this is missing.

Another obvious condition for success is this agency be a point of contact for every party in the country which needs help. It has to be organized to ease that access, and manned with enough people to meet the needs for help.

There are countless other issues: one is how to spread what the UN calls a "cybersecurity culture". A new business with a private network, opening a website may get "burned" very fast if it is not explained how to configure its system of firewalls, DMZ's and the like. The only citizens who do not need education seem to be the ones getting it the fastest: the cybercriminals. They have become extremely quick and adept to take advantage of any vulnerability whatever form it takes. New businesses in developing countries could be for them like low hanging fruits. For a cybersecurity agency in a newly cyberizing country to create conditions such that a new e-business does not get its cybersavvy the hard way by being burned first at least once, is not only a serious responsibility, but it is unprecedented.

What complicates further is the fact that different nations have different political cultures, economic structures, different priorities for the use of the internet, different geographical situations. Some are in a state of hostility with other nations and have to be concerned with information warfare. The more societies are information based, the more information warfare becomes an important component of the security equation. Some nations have more to fear from cyberterrorism than others. Critical infra-structures matter.

Any agency should be organized around its mission. So many different factors enter in the cybersecurity of each country that the mission of the cybersecurity agency will be different. To be able to accommodate this diversity is only one more challenge on the way to a more cybersecure world.

6.3 Cooperation between national cybersecurity agencies and regional agreements

Cybersecurity is inherently international. It pits all the nations of the world together. A cybercrime committed in Mexico City could have been engineered in Thailand, and the trail leading to that (when it can be reconstituted) could go via New York and Seoul (Korea). Reconstituting a trail requires the involvement and cooperation of all the nations which are part of the trail. In practice, this level of cooperation does not exist yet. It exists only partially.

Despite the fact that cybersecurity does not isolate regions, regional agreements have played a useful role, and in particular two of them: the Organization of American States (OAS) and the Asia-Pacific Economic Cooperation (APEC).

6.3.1 Latin America and the Organization of American States (OAS)

OAS has been a useful umbrella for meetings and cooperative agreements between nations of Latin America. In June 2003, the general assembly of the OAS adopted a resolution to "build and inter-American strategy against threats to computer information systems and networks". This is not to say that cybersecurity is not a concern for the future in that region. It is. Most of those nations have a very limited cybersecurity culture. But also like in most developing countries, in most of those nations, the full benefits of e-commerce for example are still to come. What these nations managed to do is to contain the cyber-criminality to acceptable levels. This is important, but this may be provisional (Paraguay for example has been mentioned as a potential problem…). Furthermore the full cyberization of the countries and their economies is still to come.

The penetration of the internet in Latin America is in average only 14.8%. Brazil perceived as one of the leaders in Latin America with a penetration of 14.1 % of the population has still room for significant growth, as can be seen from the table 2.

Table 2: Internet penetration in Latin America

LATIN AMERICAN REGION	Population	Internet Users	% Population
	(Est. 2006)	Latest Data	(Penetration)
Argentina	37,912,201	10,000,000	26.40%
Bolivia	9,281,712	350,000	3.80%
Brazil	184,284,898	25,900,000	14.10%
Chile	15,666,967	5,600,000	35.70%
Colombia	46,620,056	3,585,688	7.70%
Costa Rica	4,402,251	1,000,000	22.70%
Cuba	11,326,354	150,000	1.30%
Dominican Republic	9,119,149	800,000	8.80%
Ecuador	12,090,804	624,600	5.20%
El Salvador	6,569,953	587,500	8.90%
Guatemala	12,714,458	756,000	5.90%
Honduras	6,697,351	223,000	3.30%
Mexico	105,149,952	16,995,400	16.20%
Nicaragua	5,591,948	125,000	2.20%
Panama	3,123,055	300,000	9.60%
Paraguay	5,630,385	150,000	2.70%
Peru	28,476,344	4,570,000	16.00%
Puerto Rico	3,966,468	1,000,000	25.20%
Uruguay	3,261,570	680,000	20.80%
Venezuela	25,307,565	3,040,000	12.00%

Source: http://www.internetworldstats.com

6.3.2 Asia and Asia-Pacific Economic Cooperation (APEC) and APCERT

Countries of APEC have decided to build a group to discuss cybersecurity. This group is called APCERT (Asia Pacific Computer Emergency Response Team). Although officially under the auspices of APEC,

APCERT has a life of its own. APCERT involves 15 CSIRTs from 12 countries[37] including the US, Australia, China, but also Pakistan as well as Thailand, Vietnam, among others.

Cybersecurity is many of these countries is work in progress at an early stage of the progress. As Table 3 suggests, the penetration of the internet in Asia has still a long way to go.

Table 3: Internet Penetration in Asia

ASIA	Population	Internet Users,	Penetration
Afganistan	26,508,694	25,000	0.10%
Armenia	2,967,116	150,000	5.10%
Azerbaijan	8,388,479	408,000	4.90%
Bangladesh	136,138,461	300,000	0.20%
Bhutan	796,314	20,000	2.50%
Brunei Darussalem	393,568	56,000	14.20%
Cambodia	15,017,110	41,000	0.30%
China	1,306,724,067	111,000,000	8.50%
East Timor	947,401	1,000	0.10%
Georgia	4,435,046	175,600	4.00%
Hong Kong *	7,054,867	4,878,713	69.20%
India	1,112,225,812	50,600,000	4.50%
Indonesia	221,900,701	18,000,000	8.10%
Japan	128,389,000	86,050,000	67.20%
Kazakhstan	14,711,068	400,000	2.70%
Korea, North	23,312,595	-	-
Korea, South	50,633,265	33,900,000	67.00%
Kyrgystan	5,377,484	263,000	4.90%
Laos	5,719,497	20,900	0.40%
Macao*	490,696	201,000	41.00%
Malaysia	27,392,442	10,040,000	36.70%
Maldives	298,841	19,000	6.40%
Mongolia	2,568,204	200,000	7.80%
Myanmar	54,021,571	63,700	0.10%
Nepal	25,408,817	175,000	0.70%
Pakistan	163,985,373	7,500,000	4.60%
Philippines	85,712,221	7,820,000	9.10%
Singapore	3,601,745	2,421,000	67.20%
Sri Lanka	19,630,230	280,000	1.40%
Taiwan	22,896,488	13,800,000	60.30%
Tajikistan	6,620,008	5,000	0.10%
Thailand	66,527,571	8,420,000	12.70%
Turkmenistan	6,723,715	36,000	0.50%
Uzbekistan	26,311,197	880,000	3.30%
Vietnam	83,944,402	5,870,000	7.00%
TOTAL ASIA	3,667,774,066	364,270,713	9.90%

Source: http://www.internetworldstats.com

In most of those countries, the internet penetration is still small. Eventually it will increase everywhere. It is clear that this growth will not be homogeneous. Some nations (Myanmar, Tajikistan, Turkmenistan, East Timor, Bangladesh, Cambodia, Nepal) seem still years away from a serious internet take-off. In other nations (like Japan, Hong Kong, Singapore, South Korea, Taiwan) this has already happened. While in some (like Malaysia), this is happening. And in others (Indonesia, Philippines, Thailand,..) this is about to happen. The cyberization of all these countries, whenever it takes place, will breed cybersecurity problems at home and abroad. Indonesia, the Philippines and Malaysia, to name a few were quick to produce their share of cybercriminals. Each country is also a particular case. What sets Indonesia aside is its geography (thousands of Islands, which affect the way the infrastructure is designed), or the fact that it has a significant skilled unemployment which acts as a pool for cyber-delinquency.

Viet Nam is another particular case. It is interesting as it is emblematic of common problems in developing countries. In cybersecurity as well as in its exploitation of ICT, Vietnam is more advanced and aggressive than its neighbors Cambodia or Laos. For example in Hanoi, "Paragon Solutions Viet Nam has become the first software company in Viet Nam to achieve Level 5 of the Capability Maturity Model Integrated (CMMI), the highest"[38] . The Vietnamese government takes pride of that and tries to encourage this kind of industry. There are other evidences of cyberactivity in that country. In Ho Chi Minh City there is the "ATHENA Computer Emergency Response Centre".

Viet Nam takes cybersecurity more seriously than most developing countries. Still it was in that same country that "A survey of 2,000 users by the Hanoi University of Technology's Bach Khoa Inter-network Security Center (BKIS) showed 94 percent of computers to be infected with viruses, and 87 percent with spyware and adware".[39] And some government websites have been attacked by hackers apparently from Turkey (in fact similar experiences happen to the website of many governments).

Thailand, Philippines and Malaysia are or have been allegedly hotbeds for hacking. All these countries have ambitious ICT programs. In all cases they had to work their law enforcement aspect of cybersecurity. All these countries are more "westernized" than countries like Viet Nam or Cambodia. In all cases the cyberization is the result of a technological push together with the eagerness of the population to have internet access. These countries have high technological aspirations and in all these countries a "cybersecurity culture" is growing with the help of a variety of national agencies. What is unclear is how their cyberdefense system will adjust to the changes in the future of cybersecurity and its complexification and how well it will protect those countries from serious cyberattacks from outside.

One can safely say that it will take a long time (and probably some toils and tears) before all the countries of Asia enjoy the full benefit of the internet.

Those countries benefit from belonging to the Asian pacific Economic Community (APEC) and as a result can be members of institutions like APCERT. APCERT has a good record as umbrella for regional arrangements between cybersecurity agencies of different nations. APCERT contributes to accelerate the introduction or the spread of a "culture of cybersecurity" among those countries. Noteworthy is the role of Australia. Not only it seems to have established unique and precious ties with China (an eminently problematic country in cybersecurity), but AusCERT is credited in educating some nations like Viet Nam, Thailand, the Philippines, Indonesia, Papua Guinea. It may be that out of those efforts a level of cybersecurity adequate for these countries will emerge. In that case this will provide a paradigm to build over time a cybersecurity protection system in those countries. But this may not be sufficient.

6.3.3 Africa

Africa lags in every respect. The penetration of the internet in Africa lags significantly behind the rest of the world, as shown in table 4. Africa is not a homogeneous continent. It has some regional agreements (such as "Southern Africa Development Community" (SADC)). SADC has fourteen members: Angola, Botswana, the Democratic Republic of Congo, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, South Africa, Swaziland, United Republic of Tanzania, Zambia and Zimbabwe. They have agreed in May 2005 to

standardize their cyberlaws[40] . When it comes to cybersecurity national response capabilities, none of those countries has a lot to share with the others.

Table 4: Internet Penetration in Africa

AFRICA	Population (2006 est)	Internet Users, latest data	% Population
Algeria	33,033,546	845,000	(penetration)
Angola	13,115,606	172,000	2.60%
Benin	7,513,946	100,000	1.30%
Botswana	1,856,800	60,000	1.30%
Burkina Faso	12,113,523	53,200	3.20%
Burundi	7,909,395	25,000	0.40%
Cameroon	17,378,386	167,000	0.30%
Cape Verde	485,355	25,000	1.00%
Central African Rep.	3,268,182	9,000	5.20%
Chad	8,720,110	60,000	0.30%
Comoros	666,044	8,000	0.70%
Congo	3,672,441	36,000	1.20%
Congo, Dem. Rep.	58,731,656	50,000	1.00%
Cote d'Ivoire	19,617,714	300,000	0.10%
Djibouti	779,684	9,000	1.50%
Egypt	71,236,631	5,000,000	1.20%
Equatorial Guinea	1,102,748	5,000	7.00%
Eritrea	4,189,934	50,000	0.50%
Ethiopia	72,238,014	113,000	1.20%
Gabon	1,430,453	40,000	0.20%
Gambia	1,471,863	49,000	2.80%
Ghana	21,355,649	368,000	3.30%
Guinea	8,080,211	46,000	1.70%
Guinea-Bissau	1,460,253	26,000	0.60%
Kenya	34,222,866	1,500,000	1.80%
Lesotho	2,453,810	43,000	4.40%
Liberia	3,108,312	1,000	1.80%
Libya	6,135,578	205,000	0.03%
Madagascar	18,475,940	90,000	3.30%
Malawi	11,359,669	46,100	0.50%
Mali	10,751,139	50,000	0.40%
Mauritania	2,897,787	14,000	0.50%
Mauritius	1,280,579	180,000	0.50%
Mayotte (FR)	188,483	-	14.10%
Morocco	30,182,038	3,500,000	-
Mozambique	19,881,392	138,000	11.60%
Namibia	2,038,791	75,000	0.70%

Niger	12,226,270	24,000	3.70%
Nigeria	159,404,137	1,769,700	0.20%
Reunion (FR)	791,167	200,000	1.10%
Rwanda	8,807,212	38,000	25.30%
Saint Helena (UK)	4,893	1,000	0.40%
Sao Tome & Principe	170,319	20,000	20.40%
Senegal	10,842,622	482,000	11.70%
Seychelles	84,189	20,000	4.40%
Sierra Leone	5,093,570	20,000	23.80%
Somalia	12,206,142	89,000	0.40%
South Africa	48,861,805	3,600,000	0.70%
Sudan	35,847,407	1,140,000	7.40%
Swaziland	1,147,741	36,000	3.20%
Tanzania	37,979,417	333,000	3.10%
Togo	5,399,239	221,000	0.90%
Tunisia	10,228,604	835,000	4.10%
Uganda	27,771,997	200,000	8.20%
Zambia	11,249,789	231,000	0.70%
Zimbabwe	12,247,589	820,000	2.10%
TOTAL AFRICA	915,210,928	23,649,000	6.70%

Source: http://www.internetworldstats.com

Mauritius, Reunion, the Seychelles, Saint Helena, Sao Tome are special cases.

On the other hand, Egypt, Morocco, Tunisia and South Africa lead the way with Morocco being the only country where the penetration of the internet exceeds 10%. Many of the African countries have huge ambitions in the use of ICT for their development. Rwanda for example with funding from the World Bank is embarked in an ambitious program to develop a knowledge-based economy.

On the other hand, countries like Nigeria (1.1%) and Ghana (1.7%) have not yet started to exploit ICT very intensely and are already listed among the leaders in some forms of cybercrimes…

The cyberization of Africa may not be far. ICT is perceived by many as a way to jumpstart economic development. A variety of projects spanning a large spectrum including education, health, agriculture in addition to e-commerce and e-governance are being actively tried and developed. Exploiting the progress in hardware manufacturing, new cheaper computer platforms are being developed, customized to meet the most urgent needs of countries where most citizens cannot afford today's PCs.

The cyberization of Africa, when it takes off is bound to revolutionize the global cybersecurity equation. The arrival of additional hundreds of millions of netizens will exacerbate a problem already formidable and change the world map of cybercriminality.

Cyberization to be successful in those countries will require a significant attention to cybersecurity. An important "indicator" will be how these countries approach cybersecurity, i.e. the level of awareness of the African governments and what kind of national cybersecurity policy they follow.

7 ANATOMY OF A NATIONAL CYBERSECURITY CAPABILITY

What does an adequate national cybersecurity capability entail? How does one know that a nation has adequate capabilities? Why is this question so difficult to answer?

The US is probably the nation with the highest expertise. It is also the nations with the most serious threat and for which cybersecurity is the most complex.

In the US there would not be a consensus on the question whether the country is adequately prepared for all the contingencies it may have to face. Many would point to a variety of weaknesses. For example when the government assesses its performance in addressing its own cybersecurity, it shows a report card replete with "F". DOD, the State Department both got an "F" in the last one.

In other words, in the US the question of how cyber –ready the nation is does not have a clear answer. There is no consensus among experts and even less good ideas on how to improve the situation.

On the other hand, those who are critical of the situation as well those who gave an "F" to DOD or the State Department, know on what they base their judgment. There is a debate between experts on what should the cybersecurity policy of DOD and how it should be implemented. Experts happen to differ on some fundamentals. Furthermore it is intrinsically very difficult to implement successfully some cybersecurity recommendations on institutions as large as DOD, which have to protect themselves against so many kinds of threats, and whose cybersecurity rely on the "good behaviour" of so many people who think they have more important things to do than waste their time in endless and time consuming little precautions, and who also either underestimate their importance or simply do not understand them.

However contentious it may be there is a debate among experts and they do not debate randomly. This is probably what can be expected at best in any country: enough experts on the case, debating on what is the best course of action.

7.1 Every nation is a special case

Already a very unruly place, left unchecked, the internet would turn into an uncontrolled wild west. Since the internet is reaching every nation, cybersecurity concerns each nation. There is no exception. On the other hand, what that means concretely t depends on the nation. The internet is not only another form of telecommunication. It plays a central role in the life of cyberized nations and the internet provides the rest of the world access deep into their economic, political and cultural life. Cyberization leads to an unavoidable amount of exposure to some form of cyberthreat. It may come from within or outside of the country. In a world where the amount of malicious activity in the internet is so large that which of the two accounts for the majority of the traffic is not obvious, a nation which opts to save on cybersecurity now will have to pay (more) later.

7.1.1 The challenge of designing a national cybersecurity policy

Considering the fact that each nation is a special case, there is not much that can be said that applies to all cases and is not a truism. One universal fact is that cybersecurity has to be based on a national security policy. The articulation of a well-defined national security policy is the first step and in private companies more often than not, it turns out to be one of the most difficult and contentious. Cybersecurity is definitely not a case of one size fits all. Since the cybersecurity environment changes, the security policy underwriting it has to be adaptive. It has to be revisited permanently. This is what all large companies and institutions (private and public) do in cyberized countries. There is also a strong cognitive/learning element is that activity.

A lot of experience and knowledge has been developed on network security around private networks. It is where most of the communicable knowledge in cybersecurity probably resides. There is a lot that can be learned from it. But the cybersecurity of a nation differs in fundamental ways from the cybersecurity of a private network.

The security policy underlying the cybersecurity, examples of the World Bank (protection of data, integrity of communication, etc.) , is very different in nature from managing the security of a national infra-structure in such a way that it can support an economy and make it robust to malicious attacks, supports education, the government, the freedom and privacy of the citizens while being able to help and advise victims of cyberattacks. The situation may be different for each nation but in all cases the government has a difficult role to play.

7.1.2 Repository of cybersecurity savvy

Cybersecurity is inherently complex. The technical complexity is the most daunting one, partially because failure due to technical incompetence has serious consequences. They lead to immediate losses and damages. But projecting a sense of ineptitude invites further cyberattacks and exposes assets which could have been protected otherwise. It takes time to build adequate technical expertise.

One cannot overemphasize the need to have highly qualified technical people on the job. Computers are complex objects. What can be done with them has no boundaries. New forms of cyberattacks appear regularly. A cyberattacker needs to know only one kind of attack to wreak havoc. Defenders have to understand all the different forms of attack or be quick on the uptake. A high degree of technical expertise on the side of the defenders is not only of essence, it is also the most problematic capability to build. Where can this expertise be learned?

In rich countries in a relatively advanced stage of cyberization, the technical knowledge is distributed among many different parties, many of them private. In fact hackers are repository of a knowledge that even scholars can learn from. They organize extremely well attended educational meetings every year: the Black Hat and DefCon conferences in Las Vegas and in the case of Black Hat meetings in the Netherlands also. The response capabilities to cyberattacks are scattered and involve a large variety of people.

A lot of information circulates in a large variety of channels. Operators of ISPs through the NANOG (North American Network Operators Group) network interact more with their colleagues from competing ISPs than they do with their own bosses. Despite its name the network has members from all over the world. Through these interactions, the operators help each other manage the internet infra-structure in a way that looks seamless to the users. Seen from the perspective of those managing the infra-structure, what looks so seamless is in fact quite eventful.

Those networks of operators play a very important role in the knowledge building and in its circulation. And their exchanges are monitored by scholars who learn from them as well and also contribute to them.

There is no repository where all what is known and understood about cybersecurity is centralized and taught. Most of the experts are in fact experts in some aspect of the cybersecurity. And in most cases they are self-taught having learned mostly through experience. This situation will not change soon. Cybersecurity evolves so fast that one basic challenge is to stay abreast with new developments. Most of the cyberdefense capability resides in the world of system administrators and chief Information Officers and the knowledge they carry is based on years of experience and on the specific of their mission. What is referred to as “cybersecurity culture” in the US could be construed as the aggregation of these capabilities and information.

7.1.3 A challenge for developing countries

Developing countries in the process of cyberization will have to develop a new “cybersecurity culture” appropriate to their needs. Obviously it is not completely different from the cybersecurity culture of the rest of the cyberized world. It will have to be customized to their specific situation in compatibility with the demands for complying with international norms. This is not the largest challenge that those nations will have to face.

The process of cyberization of the economy of developing countries will make them go through a precarious phase of cyber-vulnerability before their e-sectors develop their own autonomous cybersecurity capabilities. The real challenge for them will be to manage as safely as possible the transition from a situation where the nation has not much to offer to cyberattackers in the form of juicy cyber targets into one where such targets will emerge. This is the most obvious effect of cyberization. Those countries will have to undergo a quantum jump in cybersecurity savvy to avoid having cyberattackers having a field day spoiling them from the benefits of an IT based economy before they have time to develop it. The concern is about the transition from a pre-cyberized to a cyberized economy.

Although prudence would dictate not to be prescriptive as to what is the best approach for a developing country, it seems that this calls for a national agency, whose mission would be to facilitate this transition. A national agency masterminding the whole cybersecurity policy of a country would be unprecedented. There is no model to follow. One model may be in the making in Qatar. Qatar has offered a lavish contract to the American CERT to help them set-up a national cybersecurity capability over several years.

7.2 Challenges

Not only is cybersecurity complex but it changes toward becoming more complex, not less. Not all cyberattacks are serious. Some spectacular ones looked more like successful expensive pranks than major threats to our society. Most viruses do not carry any seriously damaging payload. The worldwide "success" (measured by its spread) of the I Love You virus seems to have surprised its author, a drop out of university in the Philippines. The ultimate threat of the famous Code Red, which made the first page of the Newspapers in July 2001 was a DDOS against the website of the White House. This was never raised to the level of a major threat to the US. At best it would have had a symbolic value.

7.2.1 A worsening threat

Cyberattacks are getting more ominous. Many of them do not seek visibility. They try to be silent but deadly. When they achieve visibility, it is because they are seriously disruptive, far more than the previous generation of worms. Every day sees new worms or viruses. But in most cases they are mere variations on previous ones. Once in a while a new "technology" for worm or virus is introduced, initiating a new generation. What decides whether a worm will be successful or not is not completely understood. The new generation of worms seems to be the flash threat. These worms spread faster than our ability to mount any form of response. Slammer, the first "flash threat" grounded airplanes, incapacitated ATM machines, etc. The invention of botnets gives cyberattackers a new world of options. Given the proven imagination and ingenuity of cybercriminals on one hand and the versatility of bots and botnets on the other, it is as if botnets represented a new playing field.

7.2.2 Our limited capability to adapt

Compared with the rate at which the art and volume of cyberattacks increases, the pace at which our response capability progress seems sluggish, although so far it has eventually maintained the damage within acceptable limits. When it comes to its international dimension, the problem is different.

7.2.2.1 The painful process of internationalization

There seems to be a consensus that cybersecurity calls for a high level of international cooperation. What that entails is not as clear. And it is becoming obvious that the international dimension of cybersecurity is not taken as seriously as it should and as a result is not progressing satisfactorily.

Most developing nations are not taking cybersecurity seriously. Basic awareness of the problem is lacking. Reasons for that are easy to imagine. In most cases, the level of cyberization in those societies is low. So compared to other nations, the country has not much to fear from cyberattacks. Cybersecurity projects an impression of complexity and it is costly. In a country with tightly limited resources, one needs compelling reasons to invest in it. The reasons do not seem to be there.

To create the conditions for a change of attitude, it may take a cyber-fiasco of some sort in at least one of those countries. Then a likely scenario is that the world will witness a sudden awakening on this issue, which may spread like a contagious disease among the governments of developing countries.

The countries of the North too have the potential to act as obstacles to an adequate international cooperation. The system of governance of the internet in those countries gives a limited authority to their government in issues of cybersecurity. The governments can speak on behalf of law enforcement, but hardly on behalf of those involved in the response to incidents. Most of that activity is the purview of private companies. In the future, we may see a change in the distribution of responsibilities. This could happen if for example, critical infra-structures were targets of attacks (this has not happened yet), or cyberterrorism enters the threat spectrum (it has been a virtual threat so far). Other scenarios are conceivable involving large attacks with botnets. But we have to be prepared to see completely different scenarios, outside of the limits of our imagination.

7.2.2.2 Technical challenges to be faced by the international community

The defense against new cyberthreats will call for revolutionary technical changes. Some of those changes would have been difficult in the previous system of internet governance. They may become next to

impossible if the internationalization of the governance of the internet introduces an additional rigidity in an environment, which has become already quite stifling, when it comes to technological innovation.

7.2.2.3. Need to automatize the detection and response to worms

This is not the only contingency that the international community will have to face. Some cyberattacks like flash threats spread so fast in the whole world that they call for automatized responses, i.e. there is no time for a man in the loop. The detection and response will have to be automatized. Today the technology does not exist for that. It is at an early stage of research and development. The system of response to such attacks has to involve the whole world. This is only one example of cyberthreats whose response could require level of international cooperation unheard of so far. If as seems likely the international community through its bureaucratic representation does not display the flexibility needed, the solution will have to come from the private sector. Seen from today in all likelihood, this is what will happen.

7.2.2.4 Revisiting the fundamentals of the internet

There are some technical issues whose solution will have to involve the international community, one way or the other. One is the reform of the Border Gateways Protocol (BGP). As it stands BGP is vulnerable to cyberattacks whose effect could be no less than interrupt completely the traffic of the internet by throwing it in “black holes”, where it would be completely lost. Many other attacks are possible, or even non malicious events that could perturb the internet traffic a bit less drastically but still to an unacceptable degree. BGP is only one of a system of features that forms the basis of the internet as an international infra-structure.

A change in BGP has the potential to come at a very high cost, but not higher than the cost of not doing anything. It is another case of pay now or pay later. That somehow BGP has to be modified and made less vulnerable is a given. The internet being as international as it is, the answer to that question will affect the whole world. Among the unanswered questions are what is the best solution, who should decide that, how can one reach an international consensus on a matter at the same time so technical and complicated and also so vital to the good functioning of an infrastructure so thoroughly international?

In an ideally rational world, the debate on BGP, already large in scope, should merge with the even more fundamental debate on how to stem the root causes of cybersecurity. Up until now cybersecurity has grown as a byproduct of the growth of the internet. We are entering in a phase where the situation may be reverse, i.e. where cybersecurity concerns may influence if not dictate future developments in the internet technology.

This debate (to a certain extent already started) could deal (and probably will) with basically every aspect of the internet. It could in particular address some fundamental questions about the basic architecture of the internet. A root cause of cybersecurity is that using a computer connected to the internet puts the user in a situation of real complexity, often largely above his or her level of understanding of those issues. The internet itself, where the packets travel, is basically a passive player when it comes to security. Making the internet (with the cooperation of ISPs) more inhospitable to malicious activity would be a much desirable improvement. To implement the kind of monitoring, analysis and even manipulation of the traffic that may entail, in an infra-structure as international as the internet is bound to raise a lot of issues.

This debate is fundamental for the long term future of the internet. The technological rationality thinks in terms of new revolutionary changes however profound they may be and when applied to the internet in light of what cybersecurity has taught, it calls for questioning the fundamental premises and protocols on which the internet based. This is at odd with an international bureaucratic logic which thinks in terms of incremental changes, i.e. an internet locked in a suboptimal technology.

8 CYBERSECURITY METRICS

An information based society to be functional has to come into terms with the demands of cybersecurity. The use of networked computers offers limitless opportunities to criminals. Cybercriminality if not kept in check can trim down the benefits of cyberization to the point of basically erasing them.

Because cybersecurity is intrinsic international, every country has an interest in the cybersecurity policy of all the other countries. Because cybersecurity cannot be ignored, with the use of the internet comes an international responsibility.

International cybersecurity norms do not exist. There is no recognized metrics to measure the degree of cyber-readiness. Developing such a metrics or indicators to hold nations to would be a useful basis for an international cybersecurity order, in a world where a lot of new nations are on the threshold of joining the cyberized world.

8.1 Three "obvious" indicators

The US cyberspace is host to more malicious cyber activity than anywhere else in the world. It tops the other countries in basically any measurable indicators such as number of infected computers in all categories of infections, number of spammers, number of cyberfrauds, etc…

Still when it comes to cybersecurity, the US is seen as the state of the art, the country where the highest degree of expertise is to be found. One would be hard pressed to identify a metrics which captures US cyber savvy and translate it in quantitative indicators.

From the US government perspective, one can think of three indicators which would be considered helpful in their fight against cybercriminality.

- Does a nation have strong cyberlaws, and do they enforce them?
- Does a nation belong to the 24/7 network?
- Has the nation joined the anti-spam pact?

These indicators are easy to understand and use. Law enforcement in many countries, but in particular in advanced cyberized countries, has a lot to benefit if cybercriminals could be traced back world wide in a timely way and unlike today, they could not hope to escape prosecution with high probability.

But put together, these indicators do not come close to measure the fullness of what cybersecurity entails. They leave the real intellectual challenge untouched. The real challenge is to open the black box of cybersecurity and get a grip of what makes a country easy or difficult to attack.

Before we address this problem, we point out that the three "obvious" indicators listed above come with their share of complication. One evidence is that as of today, many nations have not joined the anti-spam pact or are not members of 24/7 network. Putting together efficient and enforceable cyberlaws is not a trivial matter for many nations with different legal culture and philosophy, as well different political systems.

The establishment and enforcement of cyberlaws world wide is a work in progress.

A variety of reasons can be invoked to explain the reluctance of some nations to join the 24/7 networks. Joining this network implies being able to contribute to trace back the malicious traffic in the country. This in turn entails having access to all the traffic crossing or originating in a nation. There are technical and political issues involved. The Internet traffic is huge. Potentially terabytes of data must be stored and one has to have the data mining capability to search them. This is the technical aspect. There are sensitive issues of privacy and individual freedom. In the eyes of libertarians, such capability opens the door to impossible abuse and history shows abundantly that whenever abuse is possible it eventually takes place.

8.2 Technical indicators

Being able to locate and prosecute cybercriminals does not come close to provide adequate protection of economic assets or other targets against cyberattacks. A society will take full advantage of cyberization only if it can control the cyberthreat. This involves law enforcement capability, but as the example of the US shows it involves mostly technical expertise.

In the US the impact of the threat of prosecution is not such an important factor in cybersecurity, not as significant as members of the government would like us to believe. Banks for example, which are under constant cyberattacks of all kinds, tend to take care of their protection themselves and very rarely report to the FBI or law enforcement agencies. In most cases they find that the cost of having the FBI penetrates in

their life under the pretext of investigating the case offset the benefit. If there is a culture of cybersecurity involved it is under the form of the information that system administrators facing similar contingencies in different institutions (even competitors), share among themselves. One would be hard pressed to find an indicator which can adequately captures this most important reason for the resilience of the US economy to cyberattacks.

The situation is superficially different but fundamentally similar in the other advanced industrialized nations. In all these nations the process of cyberization started several years ago, at a time where cybersecurity was a simpler world. In those nations cyberdefense co-evolved with the threats and yielded the present system, which defies easy description and does not inspire confidence to all for the future, but which so far succeeded in keeping the damage due to cyberattack at an acceptable level.

If the world of cybersecurity was limited to those nations, it would be complicated, but the need for "indicators" of cyber-readiness would not be as pressing as it is. By indicators of cyber-readiness we mean a measure of technical expertise, of the ability to advise the victim of an attack and help make the country and its assets difficult to attack or resilient. Opening the black box of technology is a vital component of the development of a "culture of cybersecurity", if one has in mind the developing countries. Technical indicators measure a degree of technical expertise. They have the advantage of not being politically colored and for developing countries, they have the potential to make the difference between reaping the fullness the benefits of cyberization, or failing to do so.

8.2.1 Direct technical indicators

Most developing countries enter the cyberized world ill-equipped and their governments seem at a loss to know how to start building some cybersecurity policy, other than speaking of creating a national CERT. A national CERT is in most cases a theoretical agency made of a few cyber-experts who solve the cybersecurity problems of the country. Often the notion is that a handful of experts is plenty to deal with the cybersecurity of a country.

This is not a new misconception. The history of cybersecurity in most firms started that way. The responsibility for cybersecurity was given to a very small number of individuals, with limited resources and clout. Although there is evidence that still today many firms under-invest in their cyberprotection, most firms have learned (often the hard way) to take cybersecurity more seriously. Many firms have a CIO and CSO. Their cybersecurity groups are well organized and have a lot to teach on the security of networks and how to detect and handle complicated attacks.

Developing countries are far behind in this process. They tend to under-man their cybersecurity agencies when they have one. One danger of weakening a national cybersecurity agency is that it reduces its role and eventually clout. It becomes sometimes more like a research agency, while the cybersecurity resiliency of the country grows separately within the private sector. To a limited extent it is what is taking place in Brazil.

For countries for which cyberization is hardly started, building a cybersecurity expertise in the country and giving it a prominent role is of essence.

8.2.1.1 Technical expertise

The existence of technical expertise within the country is a prerequisite to any cybersecurity readiness. Technical experts do not hide, except when they are cybercriminals. In many developing countries cybercriminals are today the best experts in cybersecurity.

Technical expertise supposes technical experts and a mechanism for that expertise to be of use in the specific country. The expertise of cybercriminals does not need to be very large. All they need to do is understand the aspect of cybersecurity relevant for the kind of cybercrime they are interested to perpetrate. There is specialization in the world of cybercriminals. Cyberdefense experts have to be generalists. They have to able to understand all the forms of cyberattacks and the technology involved in cyberdefense.

National cyberdefense experts must be real experts. They must understand the complexities of network security and there are many of them. They must also understand the difference between the need of private networks and a national internet. They must be able to advise private companies about the former, and the government about the latter.

They must keep abreast of the changes in cybersecurity, the new forms of attacks to be able to provide an informed advice to companies (private or public) connecting to the internet.

Should that expertise necessarily reside in a government agency? In most countries so far this is not the case. But when it comes to developing countries in the early stage of cyberization, it is difficult to imagine how else a real and relevant culture of cybersecurity can be introduced and grow if the government does not invest in its development.

As far as indicator goes, what matters is the presence of an "adequate" level of expertise in the country. How is the adequacy measured, other than through the control experiment of witnessing whether the country withstands successfully cyberattacks? The seriousness with which the education of the experts is approached is another indicator. Were they self taught or did they get training in a recognized educative institution?

Another indicator is how large the group of experts is and the clout they have in the country. The size of the group has to be commensurate with the need, which is different in each country.

8.2.1.2 Clear National cybersecurity policy

The internet is a disruptive technology for most countries. Cybersecurity is an unwanted complicating factor in an already complicated situation. The concept of cybersecurity policy is new or foreign to most governments. But for reasons which will hopefully be clear in the next lines, it represents a very interesting indicator of cybersecurity readiness.

In any book on how to build CSIRT (Computer Security Incident Response Team) capability, the first item is: define the responsibility of the team. The whole organization of the team and its capability depends on its mission.

Articulating a clear security policy is considered one of the most if not the most challenging moment in the responsibility of the cybersecurity of an institution public or private. National cybersecurity is no exception. The difference is that governments have a known tendency to assign broad missions in vague terms. A good cybersecurity policy has to be implementable at the national level.

The details of this policy helps those in charge of it as well as those trying to assess it appreciate the degree of maturity in the "cybersecurity culture" in that country. It is a measure of how this country is in compliance with the general assembly UN resolution 57/239 of January 31, 2003.

8.2.2 Indirect indicators

The seriousness with which cybersecurity is approached shows in the importance put in it. Is cybercriminality taken seriously? What is the role of the internet in the life of the country or its economy? Does it affects an elite or is the access easy and widespread? Is their a digital divide within the nation?

The cybersecurity savvy of nations can be detected in a variety of indirect ways. The degree of penetration of the internet gives an idea of its importance for the life of the nation. Whether most of netizens have private computers at home or tend to share them in internet cafés or otherwise because they cannot afford them, makes a significant difference to the cybersecurity equation, in a variety of ways too long to enumerate.

8.2.2.1 Indirect indicators of cyber savvy

It is possible to have an idea of how vulnerable a newly cyberized country is to cyberattacks through a set of indirect indicators.

One set of indicators refer to how well protected private networks are. Are the networks difficult to attack, i.e. do they have good firewalls, how extensive is the use of NAT (Network Address Translation), are there honeypots or evidence that attempts of cyberattacks are detected?

Another indirect indicator is how the cyberization of infra-structure is taking place. Used in the US this indicator would project an ambiguous impression. The official documents indicate a high level of awareness of the issues and even concern. But this is in stark contrast with the way the cyberization of the infra-structures of the country is actually performed.

8.2.2.2 Cybersecurity awareness

Cybersecurity awareness, a necessary prelude to cyber-readiness does not come by itself. It reflects an attitude based on experience, but also on the way the internet enters in the life of the country and its citizens..

Is cyberization encouraged? This is the case in some nations, but definitely not in many other ones.

What is the propensity of new netizens to be cybercriminals? Is that facilitated by the nature of the connection to the internet and the poor monitoring of the traffic?

Are cybercrimes subject of interest or not? Do newspapers report cyber-incidents such as viruses? Are there incentives for citizens to connect to the internet? Is the cyberization of the country encouraged or merely tolerated by the government?

Used as indicators the answer of these questions (and many more of the same kind) merely helps informing of the context of the cyberization in the country and its form.

A threat assessment is a necessary prelude for an informed assessment of whether a country has adequate "capability to counter cybersecurity-related offenses". That threat assessment is different for each country and has to be updated continuously to account for the changes in the cyberthreat environment and the changes in the nation itself.

8.2.3.3 Evidence of the dissemination of a culture of cybersecurity

Cybersecurity through its changes has a strong cognitive component. We learn through experience and this will continue in the foreseeable future. A creation of a culture of cybersecurity also means that. This applies to all countries. But this is naturally happening in the countries in an advanced state of cyberization. This may not come that naturally in the beginning in developing countries.

It is in the developing countries that the most important changes in the cybersecurity will originate. It is also them which will find cybersecurity most challenging. In the nations which have obvious difficulty to cope with the disruptive effect of the internet.

A useful indicator would measure their success in making the internet an integral part of their life. This will not happen without the parallel emergence of culture of cybersecurity, i.e. a familiarity with the issues shared by most citizens.

There is no benchmark to decide abstractly whether "the capability to counter cybersecurity-related offenses" is good enough. Building a "capability to counter cybersecurity-related offenses" in a developing country has a strong empirical component.

8.3 Preparing for the future

A debate on the internet and cybersecurity is about the future. There are serious reasons to be concerned about the future of cybersecurity. The indicators described above have severe limitations. They do not provide a basis for a lasting cybersecurity international order. Such indicators do not exist.

One obvious preoccupation is that the cyberattacks of the future will probably dwarf what we have experienced so far, but in ways we do not know for sure. So far each time a cyberthreat looks formidable, it found a kind of answer, but it was replaced soon by another one, which at first seemed even more challenging. So far a response came. But also in most cases, we discovered with hindsight that some of the previous attacks could have been more deadly. In a sense we had been lucky.

Will cybersecurity put under control and become a thing of the past, or will it like the immune system, become an important part of the life of nations?

Can an international cybersecurity order result from the cooperation of all nations sharing norms and practices? This is implicitly the assumption underlying the pursuit of indicators. But this may be a futile pursuit.

END NOTES

[1] G. Sadowsky, J.X. Dempsey, A. Greenberg, B.J. Mack, A. Schwartz: Information Technology Security Handbook, World Bank Publication, 2003.

[2] M. Dunn : A comparative Analysis of Cybersecurity Initiatives Worldwide, paper presented at the WSIS Thematic meeting on Cybersecurity, Geneva, June 2005.

[3] M. Dunn, loc.cit

[4] M. Dunn, loc.cit

[5] M. Dunn, loc.cit

[6] It is a Federally Funded Research and Development Center (FFRDC).

[7] IC4 2004 Internet Fraud – Crime Report

[8] "Smashing the stack for fun and profit" by Aleph One Phrack 49. http://destroy.net/machines/security/P49-14-Aleph-One

[9] Staniford , S., D. Moore, V. Paxson, N. Weaver, The Top Speed of Flash Worms, WORM04 October 29, 2004.

[10] America Online & The National Cyber Security Alliance. October 2004, http://www.staysafeonline.info/pdf/safety_study_v04.pdf

[11] Dan Illet, ZDnet UK, November 25, 2004

[12] http://enterprisesecurity.symantec.com/article.cfm?articleid=5213

[13] Symantec, http://enterprisesecurity.symantec.com/article.cfm?articleid=5213

[14] http://www.honeynet.org/papers/bots/

[15] David D. Clark, John Wroclawski, Karen R. Sollins, Robert Braden, Tussle in cyberspace: defining tomorrow's internet IEEE/ACM Transactions on Networking (TON), Volume 13 Issue 3, June 2005

[16] J.W Thompson, Chairman of Symantec, testimony to US Congress (November 6, 2003).

[17] www.clearcommerce.com

[18] January 2004 edition of US VeriSign's "Internet Security Intelligence Briefing" report

[19] http://www.mi2g.com/

[20] http://seclists.org/lists/isn/2004/Sep/0051.html

[21] http://news.com.com/Russian+police+Our+hackers+are+the+best/2100-7348_3-5661547.html

[22] D.Ilet, CNET News.com April 15, 2005.

[23] http://www.castlecops.com/a3834-In_Brazil_a_fine_line_between_good_guy_hackers_and_cybercrooks.html

[24] GCCCS

[25] http://www.spamhaus.org/statistics/countries.lasso

[26] http://www.antiphishing.org/reports/apwg_report_mar_06.pdf

[27] March 21 2006 incident at the site: http://www.magsecurs.com/

[28] http://www.theregister.co.uk/2006/04/26/international_phishing_survey/

[29] B. Endicott-Popovsky, D. Ryan, D. Frincke: the New Zealand Hacker case, Oxford Internet Institute Cybersafety Conference Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities Oxford University, Oxford, United Kingdom, September 2005

[30] B. Endicott-Popovsky, D. Ryan, D. Frincke: the New Zealand Hacker case, Oxford Internet Institute Cybersafety Conference Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities Oxford University, Oxford, United Kingdom, September 2005

[31] Attfield, P., Ming-Yuh Huang , "Real-World Access Control Systematic Failures: Reality or Virtual Reality," in Journal Article Workshop, June '05, Ukraine.

[32] Ref for 24/7 map

[33] http://www.prolexic.com/zr/

[34] SoBig virus

[35] http://securityresponse.symantec.com/avcenter/venc/auto/index/indexW.html

[36] http://www.lurhq.com/blackworm-stats.htm

[37] D. Nain, N. Donaghy, S. Goodman, A Survey of the International Landscape of Cybersecurity.

[38] Viet Nam News, info Byte, (26-02-2005)

[39] Than Nien news, December 29, 2005

[40] http://computerworld.com/governmenttopics/government/policy/story/0,10801,101755,00.html Accessed April 25, 2006.