CYBER RESILIENCE, CYBER DISASTER MANAGEMENT - THE WAY FORWARD

- **Abstract**

As a side effect of globalisation and massive cyber services the number of crimes both perpetrated at local and global level is growing up. Governments and Law Enforcement Agencies are aware of this and look for potential countermeasures not only following traditional solutions. Technological countermeasures are not enough there is a need to foster the Culture of Cyber Security. This paper will start setting the scene and describing the evolutionary path followed by cyber technology. Cybersecurity and the need to foster a "Culture of cybersecurity" will take us to the latest part of the document devoted to the social and economic impact of "cyber".

Keywords: *Cyber Resilience, Natural Human Disasters, Terrorism, Cybersecurity, Cyber Attacks, Culture of cybersecurity*

- **Setting The Scene**

Cyber technology is pervasive and its key role is growing up every day, citizens consider cyber technology as a commodity. Mobile devices represent the most recent revolution in both technology and society, they are perceived as something different from computers even if they play, among others, the same role and immediately became part of our daily life, a wearable accessory as our wallet or wristwatch. Extremely user-friendly devices are nowadays used by formerly digital divided citizens having no idea about potential drawbacks. As a side effect of globalisation and massive cyber services the number of crimes both perpetrated at local and global level is growing up. The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario where the malicious use of digital technologies is becoming a new business opportunity not only as a direct mean to steal "assets" and take control of smart objects but even under the format of "cyber-crime as a service", at the same time terrorists found in cyber technology the best mean both to run their activity and to enrol new "adepts".

It is common knowledge that organizations worldwide face a dangerous shortage of network security personnel that have the skills required to defend against cyber-attacks[1]. At the same time the number of breaches grows steadily, with the incident response and attack defence techniques being time-critical, as the majority of compromises (87%) occurring within minutes[2]. This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks.

[1]Keysight (2018). *Network Visibility and Network Test Products*. [online] Keysight. Available at: https://www.keysight.com/in/en/cmp/2020/network-visibility-network-test.html [Accessed 8 Feb. 2021].

[2]Verizon Enterprise. (2021). *Business Insights and Resources*. [online] Available at: https://enterprise.verizon.com/resources/?page=1 [Accessed 8 Feb. 2021].

- **Cyber Resilience?**

I won't just deal with cyber-attacks ...Nowadays "resilience" is one of the most used keywords. There are a number of definitions of resilience (accordingly with Cambridge English Dictionary):

"*The capacity to recover quickly from difficulties; toughness*"
"*The ability of a substance to return to its usual shape after being bent, stretched, or pressed*"

Nowadays, in the pandemic time, as much important as the physical meaning are the phycological aspects:
"*The ability to be happy, successful, etc. again after something difficult or bad has happened*";
"*Resilience is the psychological quality that allows some people to be knocked down by the adversities of life and come back at least as strong as before.*"ICT can play a relevant role in offering a second chance to come back.

The term resilience has as much definitions as the sectors involved, if we consider the cyber sector, cyber resilience means "*the ability to prepare for, respond to and recover from cyber-attacks*".
Even something that is perceived far from the usual idea of resilience, in the specific domain of software interfaces resilience that can be summarized as: *the system should provide some resilience to user errors and allow the user to recover from errors. This might include an "undo" facility, confirmation of destructive actions, 'soft' deletes, etc.*

- **Cyber Disaster Management**

This term is usually tightly linked with cybersecurity and cyber-attacks and express the ability to recover after a cyber disaster,a relevant cybersecurity breach that caused one or more of the typical lockdowns of cyber activities (Denial Of Service, network communication breakdown, general malfunctions, etc.). We must not forget the human factor in such situations, often the weakest link in the chain.

Typical examples were WannaCry, Petya that we all know.Through the time a number of cyber disasters have been recorded: loss of US Votes, loss of "citizens" on the occasion of census, loss of sensitive data.

- **Not only Cyber Attacks**

Cyber resilience in case of cyber-attacks is an interesting topic involving specific infrastructures, plans (governance), risk assessment and mitigation actions, CSIRT, cyber ranges exercises and more, nevertheless there are additional causes of cyber disasters.

Dealing with cyber resilience and cyber disasters it is wise to extend the possible causes to natural and human disasters, terroristic attacks, technological malfunctions and design problems, intrinsic digital fragility and more.

Some years ago, on the occasion of the WSIS Forum His E. Mr Yasuo Sakamoto, Vice-Minister for Policy Coordination, Ministry of Internal Affairs and Communications (Japan), said: on the occasion of natural disasters ICT is the lifeblood to ensure citizen's safety; and, on the same occasion, Mr. Sunil Bahadur Malla, SecretaryMinistry of Information and Communications in

Nepal, told us on the occasion of his contribution: ICTs were crucial in recovering the territory during and after the recent earthquake.
That's for sure true, the point is to ensure cyber services continuity even in the event of a disaster.This means that in addition to preventive measures addressed to face any kind of hacking attack we must put in place solutions to ensure "business continuity" even in case of other causes.

Cyber resilience in an event of disaster or terroristic attack involves an a priori identification of critical infrastructures and a specific risk analysis identifying all the potential vulnerabilities and combination of vulnerabilities. Once we have a list of specific vulnerabilities for each "node" we match them with local dangers considering both the pipeline of vulnerabilities/dangers and the cross action of different vulnerabilities/dangers on different interconnected nodes (e.g. power supply, net devices, fibreoptic,etc). to map the overall risk.

Specific solutions have been studied to overcome possible problems in case of disasters including satellite connections, deployment of emergency network nodes both wired and wireless, switchboards connecting different digital phone lines (landlines, 4/5G, UHF, CB, OM, air band, Tetra).Of course, as a key "partner" of technical solutions we must put in place a strong flexible organisation on the human side.

The recent pandemic, for instance, was a significant stress test for network infrastructure and data servers, typical approaches to the design of the network infrastructure and data servers were not sized for a mass access to the infrastructure and pervasive use of it generating huge volumes of data transfer both in and out.

The extended use of lockdown boosted the access to on-line services ranging from government offices to on-line shops to buy goods and receive food and drinks at home including a massive use of music and video streaming throughout the whole day.

An additional must is to ensure as much as possible business continuity enabling, when applicable, on-line working sessions, many times this requires video conferencing tools to enable many to many interactions.

All these activities require an adequate network infrastructure ensuring enough bandwidth ideally to all the internet users connected in audio-video streaming, a similar situation it is not foreseen by the actual technical specification so to do not collapse the network the bandwidth must be carefully used,for instance, switching off video connections on conferencing platforms.

Similar overcrowding problems can affect interaction with e-services, for instance, e-Gov services resulting in a Denial Of Service (DOS) many times due to the inadequate servers.

These problems are usually due to architecture design specifications not to technological limits; a number of global platforms having an adequate network connection and server farm use to operate properly even in case of global "Black Fridays".

Drawing some conclusions, cyber resilience is already a must since we "moved" in the cyberspace a number of critical services. Resilience under cyber-attacks is a paramount, it is a "glocal" problem to be solved both at global level because national cybersovereignty does not lock cyber frontiers at the same time on local level a number of well-defined infrastructures and actions must be activates, a tight cooperation among states must operate.

Cyber resilience in an event of disaster or terroristic attack involves a far wider range of protection measures, as already described, an a priori identification of critical infrastructures and a specific risk analysis identifying all the potential vulnerabilities and combination of vulnerabilities.
Considering the trend toward smart-home / cities / energy / mobility the risks due to the merge of cyber technology controlling a number of infrastructures is far higher than in the past.

- **Cyber Ranges**

A Cyber Range provides a simulated environment to conduct tests and rerun exercises to enhance cyber defence technologies and skills of cyber defence professionals, in addition their simulation features will offer a global situational awareness on the risk-chain and related attack surfaces.

These platforms provide tools to test the resilience of networks and systems by exposing them to realistic nation-state cyber threats in a secure facility with the latest tools, techniques and malware, this facilitate the testing of critical technologies with enhanced agility, flexibility and scalability, it helps to strengthen the stability, security and performance of cyber infrastructures and IT systems used by governments and private organisations.

These platforms enable to conduct force-on-force cyber games/exercises, cyber flags; provide an engineering environment to integrate technologies and test company-wide cyber capabilities, cybersecurity technologies, and customer and partner capabilities, along with the testing and demonstration of cyber technologies to test existing and future mission-critical systems against cyber-attacks.

On the training side cyber ranges will offer to cyber professionals the opportunity to develop the skills facing a relevant number of cyber-attacks and their overall impact. A cyber range allows organizations to learn and practice with the latest techniques in cyber protection, practitioners will be able create and test different strategies customizing sophisticated testing protocols in short time. As a follow up of the training session practitioners, after the result of their countermeasures may receive suggestions on the best practice in the specific situation as identified by the platform or retrieved in the knowledge base.

Main outcomes obtained thanks to cyber ranges are: improved situational awareness of cyber warfare scenarios, rapid identification of zero-day vulnerabilities, environment for the development of countermeasures, training environment for practitioners.

Communication networks can deeply influence a relevant number of services and the combined effect of such effects may led to serious and sometimes unpredictable consequences.
There is a need to develop an international/global Cyber Range Network to share knowledge and information enabling an improved approach to countermeasures and tactics. Cyber Ranges are designed to easily create virtual environments devoted to cyberwarfare training and cybertechnology development. Such platforms, in line with typical simulator’s features, are fed by real case study and create a knowledge base of cyber threats, related extended effects and mitigation/counteractions. A specific useful feature to be incorporated is the identification of the zero-day vulnerabilities in order to reduce or eliminate the Window of Vulnerability (WoV) and identify main attack vectors.

- **Europeans Cyber laws**

Since 1996 a number of countries decided to enact cyber laws. On 23 November 2001 the Council of Europe issued the European Treaty Series No. 185 entitled "Convention on cybercrime". Some of the paragraphs are devoted to: Illegal Access, Illegal interception, Data interference, System interference, Misuse of devices, Computer-related forgery, Computer-related fraud, Offences related to child pornography, Offences related to infringements of copyright and related rights, Attempt and aiding or abetting.

European societies are increasingly dependent on electronic networks and information systems. The European Commission considered, since the announcement of the "Information Society" model, cybersecurity as an enabling tile of such a model, protecting from criminal activity what threatens citizens, businesses, governments and critical infrastructures alike: cybercrime.

Cybercrime is borderless and could be ubiquitous, committed even thanks to a mobile phone. In order to combat cybercrime a number of actions are required: legislation, specific law enforcement units, active and passive protection, education – a "culture" of cybersecurity and more. The European Union has implemented legislation and supported operational cooperation, as part of the EU Cybersecurity Strategy released in 2013.

Later on, in 2017 the Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" builds on and further develops the EU Cybersecurity Strategy. As outlined in the Communication (2017), the European Commission continues to work on effective EU cyber deterrence, by, among other actions, facilitating cross-border access to electronic evidence for criminal investigations. If we focus on evidences it is evident that "traditional" physical evidences may be collected in a proper way and safely stored in warehouses; digital evidences are quite different; they are often distributed on line and hosted by different organisations and servers, in addition they are "fragile" and may disappear[3] along with elapsed time. A specific problem is due to privacy issues and trust relations between IT (hard and soft) companies and customers. As an example, let's consider smart phones or social media companies; they protect the privacy of their own customers so many times, they do not provide access to specific potential criminal content to law enforcement agencies. Here comes the eternal fight between security levels implemented by companies (telecom, social media, etc.) and governments; governments must be few steps forward and have potential access to private information to keep restricted information undisclosed and ensure citizens' safety and security.

As a specific European law enforcement agency fighting cyber-crimes the European Commission has played a key role in the development of European Cybercrime Centre (EC3[4]), which started operations in January 2013. EC3 is part of Europol[5] and "acts as the focal point in the fight against cybercrime in the Union, pooling European cybercrime expertise to support Member States' cybercrime investigations and providing a collective voice of European cybercrime investigators across law enforcement and the judiciary."

[3]Simplyconsiderdigitalpreservationaspects.

[4]Europol. (2020). *European Cybercrime Centre - EC3*. [online] Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [Accessed 8 Feb. 2021].

[5]Europol - European Union's law enforcement agency. (2020). *Home*. [online] Available at: https://www.europol.europa.eu/ [Accessed 8 Feb. 2021].

Back to national approach to cyber laws, we will consider the Chinese approach to cyber technology introducing the "Cyber Sovereignty" approach. A similar overall approach is shared with India[6] as well. The Indian Parliament enacted the Information Technology Act 2000 (ITA-2000) on October 2000; it was the first law in India dealing with cybercrime and electronic commerce. The reference model of ITA-2000 is the United Nations Model Law on Electronic Commerce 1996 (UNCITRAL Model).

On July 2017 The Times of India published an article entitled "One cybercrime in India every 10 minutes"; according to the Indian Computer Emergency Response Team, 27,482 cases of cybercrime were reported from January to June 2017. These include phishing, scanning or probing, site intrusions, defacements, virus or malicious code, ransomware and denial-of-service attacks. In order to favour the report on cyber-crimes, on April 2017, the Ministry of Electronics & Information Technology (MEITY) published in the International Journal of Science Technology and Management a specific article entitled "How to report cyber-crimes in Indian territory". New Delhi hosts since 2014 the International Conference on Cyber Law, Cyber Crime & Cyber Security, a key international event organised and chaired by Pavan Duggal, Advocate at the Supreme Court of India, world-class expert in this field.

Estonia has invested time and resources to develop a sound regulatory framework in the field of cyber. Germany decided to focus mainly on critical infrastructures protection while Russia promoted the idea that Russian data must reside on the Russian territory. To conclude this excursus on cyber laws we may include two more countries like Bahrain and Zimbabwe; they both developed specific cyber laws. On 12 February 2015 Bahrain enacted the new cybercrime law; it seeks to reduce crimes by establishing penalties to protect public interest. Under the law is considered a criminal: anyone who gets illegal access to an IT system or part of it, anyone threatening to cause damage for personal gains, anyone convicted of entering, damaging, disrupting, cancelling, deleting, destroying, changing, modifying, distorting or concealing IT device data concerning any government body, anyone convicted of embezzlement of funds, receiving favours for oneself or others, forging documents. For online distribution of pornographic material, the sentence is doubled if the pornographic material targets children.

An additional short list of what kinds of activities are considered computer crimes may include but it is not limited to:

- Improperly accessing a computer, system, or network;
- Modifying, damaging, using, disclosing, copying, or taking programs or data;
- Introducing a virus or other contaminant into a computer system;
- Using a computer in a scheme to defraud;
- Interfering with someone else's computer access or use;
- Using encryption in aid of a crime;
- Falsifying email source information; and
- Stealing an information service from a provider.

While bullying, sexual harassment, and child pornography are long-standing crimes and societal problems, the Internet and social network sites have introduced a whole new arena for predators to

[6]WSIS Forum 2017 | Information and Knowledge Societies for SDGs (2017). *WSIS Forum 2017*. [online] WSIS Forum 2017. Available at: https://www.itu.int/net4/wsis/forum/2017/Agenda/Session/254 [Accessed 8 Feb. 2021].

practice their trade. These last three crimes are expanding due to the Internet; so far, they represent a typical issue for cyber-laws.

A synthetic description of Cyberbullying is: aggressive harassment that occurs using electronic technology, including cell phones, tablets, and computers using social media sites and chat sites. Cyberbullying includes the sending of unwanted, abusive text messages, photographs, personal information, defamatory and libellous allegations and rumours, and the creation of fake profiles intended to harm victims. Child pornographers and child molesters have unfortunately found the Internet to be a useful tool to prey on children as well.

In the United States the Department of Justice has a special task force devoted to catching these predators, and if your child has been targeted, you should contact law enforcement right away. The Department of Justice has published a Citizen's Guide to Child Pornography to outline the laws and your remedies. Victims should report the crime to parents, network providers, schools, and law enforcement. Hate crimes are the most heinous of the various cyberbullying crimes, and they carry their own distinct set of penalties in most states, including additional jail time and sometimes mandatory prison time if connected to another felony. Hate crimes also pique the interest of the FBI, which prosecutes hate crimes and maintains statistics on the proliferation of hate crimes and other forms of civilian terrorism. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, published by Cambridge University Press, is the most comprehensive analysis of how existing international law applies to cyber operations. The drafting of the Tallinn Manual 2.0 was facilitated and led by the NATO Cooperative Cyber Defence Centre of Excellence[7].

- **Closing remarks**

To conclude let's recap the key points outlined within this paper, cyber technology is nowadays pervasive and at different level present all-over the globe, digital data creation in the different formats (text, graphic, audio, video, etc.) are growing exponentially,as a consequence of the tight relation between cyber technology and our everyday life. A significant investment in digital literacy starting from primary schools is a paramount, young generations are exposed to many threats because of their intensive use of technologies without and adequate knowledge of potential drawbacks and risks. The capillary presence of "extreme" user friendly cyber-devices enabled "digital divided" citizens, not aware about potential risks, to access the cyber-world.

Cyber security together with cyber laws, when necessary, are a pre-condition to safely exploit e-Services. E-Government, e-Business or e-Health are in danger and may act as bad ambassadors if cyber security is not ensured technically and legally.

At global level the malicious use of cyber "troops" may design a credible warfare scenario reserving traditional warfare scenarios to minor local conflicts still based on conventional weapons. In such an actual and future scenario on the defence side it seems a must to maximise the potential of cyber defence, one of the opportunities is offered by Cyber Ranges both to assess cyber infrastructures resilience, test new countermeasures, launch force to force and cyber flags exercises and last but not the least active training of practitioners.

[7]Ccdcoe.org. (2021). *CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise.* [online] Available at: https://ccdcoe.org/ [Accessed 8 Feb. 2021].

Apart from pure cyber defence there are some other relevant actions to intercept potentially dangerous trends, future threats and more. One of the main approaches to act "ex-ante" thanks to the pervasive role of digital technologies and related data exchange is the advanced in-depth analysis of big data streams, social media, open source intelligence, socio-economic and geo-political factors, human factors, potential influencers, crowd sourcing, and remote sensing. This task will be carried out thanks to enhanced data analytics, machine learning and artificial intelligence.

In conclusion we are already in the arena of cyber "warfare" where troops, tanks, ICBM, choppers are the "cleverest" bit and bytes assaulting or defending our resources and life style. To extremely simplify the basic scenario, it is not conventional war, it is not guerrilla warfare, it is not terrorism where one single man can create relevant damages somewhere, it is a new treat in which one single man located anywhere can create relevant damages globally.

- **Bibliography**

1) Babel C (2015) Tackling privacy concerns is key to expanding the internet of things, Wired Innovation Insights, Feb 2015
2) Critical Link is building a network of volunteer emergency First Responders, who are dispatched through SMS and Mobile alert to save lives when people are injured in Dhaka. https://play.google.com/store/apps/details?id1⁄4com.ionicframework.critical ink453552
3) Damico Tony M (2009) A brief history of cryptography. Inq J 1(11): 1/1, 2015 Student Pulse. All rights reserved. ISSN: 2153-5760
4) Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inf Theory 22 (6):644–654
5) Duggal P (2018) Cyber Law 3.0, LexisNexis, Gurgaon, India, ISBN 978-81-3125-366-3
6) European Commission (2017) Resilience, Deterrence and Defence: building strong cyber-security for the EU, JOIN (2017) 450 final
7) Fyffe S, Abate T (2016) Stanford cryptography pioneers Whitfield Diffie and Martin Hellman win ACM 2015 A.M. Turing Award, Stanford News Service, Stanford University, Stanford, CA
8) Grillo (Cricket) – Grillo's alerts will tell you when the earthquake will arrive and how strong it will feel where you are. http://grillo.io
9) High Representative of the European Union for Foreign Affairs and Security Policy (2013) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final
10) Kahn D (1997) The Codebreakers: the story of secret writing. Scribner, New York. ISBN:978-1-439-10355-5
11) Milanov E (2009) The RSA algorithm, accelerated (honors) advanced calculus. University of Washington, Seattle
12) NATO Cooperative Cyber Defence Centre of Excellence (2017) Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press
13) Ompall, Pandey T, Alam B (2017) How to report cyber crimes in Indian territory. Int J SciTechnolManag 6(04), April 2017, ISSN 2394-1537
14) Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, http:// workspace.unpan.org/sites/Internet/Documents/UNPAN96078.pdf
15) Ronchi Alfredo M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry , ISBN 978-3-030-00746-1, Springer (D)

16) Ronchi Alfredo M., WSIS Forum 2015, High Policy Statements. https://www.itu.int/net4/wsis/forum/ 2015/Content/doc/outcomes/Policy_Statements_Booklet_WSIS2015.pdf
17) Ronchi Alfredo M., Duggal P et al, WSIS Forum 2016 Outcomes. https://www.itu.int/net4/wsis/forum/ 2016/Outcomes/
18) Ronchi Alfredo M., (2019), e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01596-1, Springer (D)
19) Ronchi Alfredo M., (2019), e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)
20) Ronchi Alfredo M., (2018), Cybertechnology: Use, abuse and misuse, ISBN 978-5-91515-070-X, UNESCO IFAP Interregional Library Cooperation Centre – Moscow, Moscow, Russian Federation
21) Ronchi Alfredo M., (2018), 21ST Century Cyber Warfare, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018
22) Ronchi Alfredo M., (2018),, TAS: Trust Assessment System, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018
23) Ronchi Alfredo M., (2018), Hybrid treats: defence line from the grassroots, NATO STO Issue no. 3: Defence Technology Foresight, Bulgarian Defence Institute, 2 Prf. TsvetanLazarovblvd. Sofia, Bulgaria
24) Ronchi Alfredo M., (2018), High-level Track Facilitators (HLTFs), WSIS Forum 2018: High-Level Track Outcomes and Executive Brief, ISBN 978-92-61-25171-0, pag. 3,6 © ITU, International Telecommunication Union ITU, Geneva, CH
25) Ronchi Alfredo M., (2018), . . .1984 won't be like "1984"?, ISBN 978-5-91515-068-9, Interregional Library Cooperation Centre, Moscow
26) Ronchi Alfredo M., (2018), Thematic Workshop: ICTs for Safety, Security and Disaster Recovery, ISBN 978-92-61-25151-2, International Telecommunication Union ITU, Geneva (CH)
27) SAS report on The Internet of Things. http://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html
28) Thawte (2013) History of cryptography, an easy to understand history of cryptography. Thawte
29) Thiesmeier L, Capture and readiness of slow-onset disaster information in Southeast Asia. https://www.itu.int/net4/wsis/forum/2016/Content/AgendaFiles/ document/7ea0c767-3a4b-40fe-8a30abd09b80c666/5_THIESMEYER_WORKSHOP_172.pdf
30) UNESCO (2014) Human development report 2014. Sustaining human progress: reducing vulnerabilities and building resilience
31) Virgo – Safety device for the protection of operators working in risky environment. http://www. intellitronika.com/virgo/