IST-Africa
IST-Africa 2019 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2019
ISBN: 978-1-905824-62-5

Fostering the Culture of Cyber Security

Alfredo M. RONCHI
Politecnico di Milano, Piazza Leonardo da Vinci 32, Milano, 20133, Italy
Tel: +39 02 2399 6040, Mob: +39 393 0629373, Email: alfredo.ronchi@polimi.it

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. The present paper introduces an innovative Cyber Range to be integrated in the foreseen European Cyber Range Network. The proposed solution provides 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 cyberinfrastructures and IT systems used by government and private organisations. The document describes a platform devoted to easily create virtual environments devoted to cyberwarfare training and cybertechnology development. The solution is in line with typical simulator's features will be fed by real case study and will create a knowledge base of cyber treats and related extended effects and mitigation /counteractions. A specific features is the identification of the zero-day vulnerabilities in order to reduce or eliminate the Window of Vulnerability (WoV) and identify main attack vectors.Main outcomes are: improved situational awareness of cyber warfare scenarios, rapid identification of zero-day vulnerabilities, environment for the development of countermeasures, training environment for practitioners.

Keywords: Cybersecurity, Culture of cybersecurity, ethics, privacy

1. From Vision to Reality

Thirty years ago, information scientists and computer users witnessed the unprecedented revolution due to personal computing[1]. This revolution was initiated by visionary researchers like Douglas Engelbart[2] and his "oN-Line System[3]" that is directly connected with "The Mother of All Demos", as retroactively termed its presentation at the IEEE on 9 December 1968, to do not forget the concept of a revolutionary device: the "mouse"; Butler Lampson, Charles P. Thacker, Robert W. Taylor and Alan C. Kay licensing in 1973 the Alto[4] computer and its object oriented interface ten years before Apple Macintosh[5]. In the 1980s Alan Kay, developing "Dynabook", introduced the concept of laptop computer.

[1] The "Homebrew Computer Club" was a "club" of computer hobbyists founded in the Silicon Valley in 1975, they use to meet and present their achievements. This group and the atmosphere of the time is well depicted in the movie "Pirates of Silicon Valley" (1999 Turner Network Television) based on Paul Freiberger and Michael Swaine's book "Fire in the Valley: The Making of the Personal Computer".

[2] On the occasion of the WWW 1997 Doug Engelbart introduced the concept of a "multidimensional" operating system showcasing a graphical interface associating each single process to a "dimension" of a n-dimensional interface.

[3] Developed by Douglas Engelbart and Dustin Lindberg at SRI International.

[4] Xerox Alto had a limited diffusion on the market, in the 1980s Xerox created Star a modified and cheaper follow-up of Alto.

We are witnessing relevant changes due to both technological enhancements and modification of user requirements/expectations. In recent times the digital domain, once strictly populated by professional users and computer scientists, has opened up to former digitally divided. Technology is evolving toward a mature "calm" [1 - Weiser 1991] phase, "users" are overlapping more and more with "citizens" [2 - Council of Europe 2001] and they consider technology and e-Services [3 – Ronchi 2019] as an everyday commodity, to buy a ticket, to meet a medical doctor, to access the weather forecast. 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. Starting from the first decade of the twenty-first century a relevant number of Governmental Agencies, Institutions and Private Enterprises spread all over the world both in industrialised and developing countries invested time and resources on e-Services.
As a side effect of globalisation and massive use of cyber services and the "appification" of society the number of crimes both perpetrated at local and global level is growing up.
Current digitisation of almost everything including security and government services has created increased vulnerability to cyber-attacks Governments and Law Enforcement Agencies are aware of this and look for potential countermeasures not only following traditional solutions. The more we become digitalised, the more we are vulnerable to hackers.

2. Objectives: A Culture of Cyber Security

Cyber-security was one of the first aspects to be improved since the inception of the "Information society" idea. Of course, any kind of on line activity must be managed in a secure way or at least, as we will see, at a certain level of "insecurity". Quoting Salman Rushdie, "There is no such thing as perfect security, only varying levels of insecurity."

The gap between e-Citizens and digitally divided citizens has not disappeared yet but is becoming smaller every day. In the near future young generations [4 - Ronchi 2010] will not figure out how their parents used to fulfil some tasks in the past.
We all discussed for quite a long time about the potential problems due to the so called "digital divide", the goal was and still is to bridge the gap between digitally savvy and the "analog generation" on one side and the creation of a proper digital infrastructure.
These efforts were mainly devoted to basic capacity building in the use of digital technology and more specifically e-services to ensure the shift from traditional interaction, mainly human mediated to digital interaction. Citizens use to prefer to go to the front desk or use the telephone. In the 1990s the problem related to the digital infrastructure and more in general to the access to the Internet started to be partially solved thanks to some telecom players that breaking the rules offered phone free access to the Internet, this approach later evolved to ISDN flat rate connections.

Having positively solved Internet access the next true revolution was ignited by mobile position-aware devices. Smart phones before and immediately after tablets, two kinds of "non-computer" devices enabled mass access to e-services. "Non-computer", yes; one of the last barriers was the approach to "computers", the inherited idea of complexity and high skills requested in order to use and not damage them; smart phones and tablets [4 - Ronchi 2010] were not perceived as "computers", they are something different, friendlier, more personal. In few words, you don't need to think "do I need to take it with me?"; it is like your wallet, you take it!

[5] Steve Jobs understood the relevance of that revolutionary approach to computing and activated Lisa and later Macintosh projects.

These devices together with mobile connectivity turned citizen into e-citizens but a relevant problem wasn't solved like cybersecurity and privacy issues. These aspects are particularly sensitive with reference to young generations and kids, nowadays already on line.
It is a common understanding that recent generations [5 – Jones 2011] represent a discontinuity compared with past ones. Such discontinuity or if preferred singularity is recognised both by adults complaining because their children do not pay attention or are getting bored by learning and by adults that have discovered new skills and capabilities in young generations [2 - Council of Europe 2001].

We used to think about the day after tomorrow, skipping today and tomorrow; network infrastructure is there, there is a bunch of useful software tools and APPs addressed to citizens, tablets and smartphones have overturned the scenario but it is evident there is a gap to be bridged; how many citizens are aware about potential cyber risks?

In a society everyday more dependent from cyber technology there is a clear need to improve awareness about potential the risks in the cyber universe. The main objective is to bridge the second gap, after the digital divide we need to bridge the cultural divide concerning cybersecurity. If cybersecurity was a prerequisite to promote home banking and e-Commerce nowadays we need to ensure a "culture" of cybersecurity to avoid a bad ambassador effect extended to the whole sector of e-Services. This task is even more relevant than the efforts devoted to bridge the digital divide, the cultural divide is more critical. This need is particularly relevant in case of young generations, the risk to be victims of different types of criminal actions is relevant: cyber bulling, blackmails, extortions, etc.

3. Methodology: Awareness, Education and Live Training

The foreseen methodology is based on both awareness, education and live training. This methodology has been promoted on different occasions including the cybersecurity track of the World Economic Forum held in Davos, some degree and post-degree courses at Politecnico di Milano. The first action to be performed is to improve awareness about potential direct and indirect risks due to improper use of digital technology.

3.1 Awareness

Some people probably consider cyber space as a kind of "outer space" no man's land not subject to humans' material desires and malicious behaviours. Voluntary or involuntary personal data dissemination is not a new phenomenon; before the Internet it was less evident and limited to some specific domains: credit card companies, travel agencies, real estate companies, car dealers, etc., basically people officially owning your personal information being in a position to suggest new opportunities or anyway reuse your personal data for different purposes. Later on, it was the time of "fidelity cards" and the explosion of CRM[6]. The mass diffusion of the Internet ignited the real blast of personal information collection and data harvesting. You fill up a form to install a new APP and suddenly you receive a bunch of offers and advertisements often claiming that you subscribed to that service. Yes, you subscribed to the form to install the APP but thanks to a kind of letter chain the company in charge of collecting the forms to install the APP is the same company that manages dozens of business companies and you unintentionally subscribed to the "full" service. Your personal information is now shared among a number of companies and you will never be sure that they will disappear from on-line data base[7]. This last aspect, "never

[6] Customer Relationship Management.

[7] We will not analyse the impact of GDPR on the above mentioned aspects in the present paper, refer to Ronchi, A.M.(2019), Toward a New Model of (Inter)active Citizenry

disappear", takes us to another relevant point. Introducing the concept of data ownership, we make reference to the copyright concept. If my data is mine I can delete it, can't I?

Privacy is concerned with control over information, who can access it, and how it is used. Privacy has many dimensions, from concerns about intrusive information collection, through the risks of exposure, increased insecurity or interference in their decisions that individuals or communities are subjected to when their 'private' information is widely known. Privacy is generally linked to individuals, families or community groups, and is a concept that is often used to demarcate a line between a 'private' and 'public' sphere.

Information is built on top of single or aggregate of data; for quite a long-time people used to think that cyberspace is a "black hole" without memory where you pour data without any side effect. Young generations shared on line sensitive information in order to access a videogame or chat with friends or, more recently, posted images and clips about their private life. In the "Appification[8]" era there are almost no limits to data collection and reuse, "someone" knows exactly where you are now and where you have been, APPs may collect your medical data, or fitness program, your expenses, or collect and analyse your contacts, your photos or video clips. In recent times crowd data collection, open and big data, more or less anonymised, has provided the big framework.

We live in a world in which there are already countless sensors and smart objects around us, all the time. The car we drive, the phone in our pocket, our wristwatch, the clothes we wear, are smart and connected; then the concept of "private" becomes far more ephemeral. This is not enough; what it is not collected by APPs will be collected in a seamless mode by IoT [6 – Babel 2015]; of course, IoT will add a lot to our life but this will cost us a significant part of our privacy. In a single generation, we witnessed the evolution of information technology from mainframes, exclusive patrimony of space agencies and super-calculus centres, to owning in our pockets a device ten thousand times more powerful, capable of observing and recording video, audio, location, and motion. These devices can communicate with nearly any other digital device from household appliances to cars. Collectively we have the ability to store, access, and process more data than humanity has created in its entire history. The actual "visual" trend is producing an incredible amount of photo/video documentation of our everyday life; does this mean "goodbye privacy?" [7 - Google]. Starting from all these aspects we will deal with main features concerning ownership, moral rights, privacy, ethics, legal framework, security, even OSINT and more.

3.2 Owning Information

The concept of "data" as it relates to people's everyday life is still evolving [8 – Burrus 2014]. We inherited the concept of copyright and we more recently faced the concept of privacy [9 - Merriam Webster].

Copyright and privacy; it seems reasonable that both derive from the concept of data ownership. we take a picture of an agreeable landscape, add our name as the author/owner on it and publish it on our web page; if someone else downloads our picture, crops the author's name and posts it on his/her website, it's a copyright infringement. Nowadays open data is one of the buzzwords most popular; if a public authority will release different sets of "open data" apparently anonymised, the combined use of them may lead to identifying your personal behaviour; that's a form of privacy invasion or perhaps violation [10 – Darrow 2016].

Historically speaking, the idea of even owning information is relatively new[9]. The earliest copyright laws, which granted the creator of artworks, among the other rights,

[8] Kind of neologism stressing the incredible proliferation of APPs.

[9] My data belongs to me, http://wsa-mobile.org/news/my-data-belongs-me-wsa-roundtable-discussion-personal-data-virtualisation-society-wsis10-review

exclusive rights to duplication and distribution of said work, first appeared in the early 18th century. Nevertheless, it would still be hundreds of years, however, before the concept of "data" as we understand it even began to develop.

The world we contributed to create, filled up with cutting edge technologies and fully connected, take us to a simple, even if uncomfortable to hear, truth: we are unable to prevent all possible data tracking. Cameras, satellites, sensors and software virtually everywhere ensure that, no matter how much technology you eschew, someone can get some data off of you. Your credit card company "tracks" your purchases and, in one word, your life-style. Your phone carrier "tracks" your calls, social relations and geographic location. Your area's law enforcement tracks the roads and intersections you walk through or drive down every day. Local administration CCTVs or private safety cameras follow you within shops or residential buildings, even inside the elevator.

Unless we decide to move to the mountains, renouncing to today's technology, some tiny data that describes our behaviour and us will probably be tracked. No matter, you may say, we have nothing to hide, but what about the use, abuse or misuse others may do?

If we specifically refer to the intellectual property from the "continental" standpoint apart from the "economic" rights we find, even more relevant, some moral rights like paternity, adaptation, modification, … "withdraw". The author has the moral right to "withdraw" his work of art from private or public environment. If we keep the similarity in the field of personal data we must claim for the right to withdraw them from the "digital universe"; this right is usually termed "right to obsolescence" or the "right to be forgotten". Viktor Mayer-Schönberger, the author of "Delete: The Virtue of Forgetting in the Digital Age" [11 - Mayer-Schönberger 2009], traces the important role that forgetting has played throughout human history. The book examines the technology that's facilitating the end of forgetting: digitization, cheap storage and easy retrieval, global access, multiple search engines, infinite replications of information, etc. If it is true that our ancestors survived the evolution process because of their ability to transfer to future generations relevant information thanks to primitive forms of writing, the dangers of everlasting digital memory, whether it's outdated information taken out of context or compromising photos, the Web won't let us forget, as is well evident and already creating troubles. The supporters of a "natural" approach propose an expiration date for digital information or a progressive vanishing of data as it happens in the human world. Other experts propose to applying the moral right of the author/owner to "withdraw" his data, and here comes the first crucial point: author, owner or subject…? A vanishing memory offers the ability to make sound decisions unencumbered by the past, offers the possibility of second chances. This is a sintesys of the first step, awareness, citizens and especially young generations must be aware about potential drawbacks due to cyber technologies. Next step is to educate fostering the culture of cybersecurity.

3.4 Education: The Culture of Cybersecurity

Once the awareness process is activated and the interest to improve knowledge about cybersecurity raises it is time to provide the fundamentals on cybersecurity. Education is the next action to be performed in order to fertilize the seed of the culture of security since primary schools and in the transition phase ensure proper education to citizens. As a direct consequence of some recent mass cyber-attacks like Petya, WannaCry, Andromeda and a number of Cryptominers some countries decided to foster the culture of cyber security from the grassroot, primary schools included.

More in general Governments should invest in media information literacy, critical thinking, security, cyber-privacy and info-ethics. If a proper merge of official curricula must join the required knowledge in the field of security the approach to proper educate

citizens must be based on effective methodologies suitable to the target audience (kids, teenagers, adults, etc.). With specific reference to universities, cyber-security courses already included in existing curricula have been improved and new post degree and continuous education courses are now available. Digital technology may help offering from edutainment Apps as experienced by the Italian Police to video reels to be enjoyed anywhere anytime. In addition an increasing number of universities designed and activated on line courses providing the key concepts to setup a first "defence line" against cyber-crimes, such courses are now compulsory for both students, professors and administrative personnel.

Cyber-security is a paramount issue to enable the fruitful implementation and adoption of e-Services from e-Government to e-Health. The World Summit on the Information society devoted since 2005 a specific action line "Building confidence and security in the use of ICTs" [12 – UN General Assembly].

3.5 Risk Assessment: Mapping

To better focus the efforts to ensure proper use of ICTs it is useful to perform risk assessment. We all know that security and privacy are subject to risk, as already stated; thus, it is important to identify and mitigate risks associated with privacy and security concerns. In order to reach this goal, as a first approach, we can perform the following steps: identify the persons at risk in the event of personal information exposure (not restricted to the data owner or collector); identify knowledge assets that can be extracted from the data collected (discrete data points, meta-analysis of data points; mash up of the collected data and external data sources); evaluate the importance of each knowledge asset to the potential goals/harms (little or no relevance, significant relevance, crucial). This approach, many times, will lead us to identify the crucial nodes that, if adequately protected, will ensure no harm. The level of privacy risk will be dependent on the likelihood that identification could occur from the release of the data and the consequences of such a release. Anyway, mitigation is many times linked to de-identification.

In the previous paragraph, we mentioned not only privacy but even security. Security, somewhat linked to privacy, adapts security protocols and tactics to encompass:

- Digital information security;
- Physical and operational security;
- Psychosocial well-being required for good security implementation.

Nowadays the key concept is "holistic security", a "global" approach to security integrating all the different aspects and problems. A specific interest is devoted to digital security. Digital security is more than focus on software or tools, integrating emotional well-being, personal and organizational security. Good implementation of digital security tools and tactics requires attending to the practitioners' psychosocial capacities to recognize and respond dynamically to different threats to them and to participants related to project data collection and communications (intimidation, social engineering).

4. Technology: Live Training

Awareness and educational initiatives must be planned to provide a significant contribution to bridge the "cultural" gap. Live training actions may be based on Cyber Ranges a typical solution to train[10] and test cybersecurity measures and exercise professionals as described in the following paragraph devoted to technologies. 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. At the same time the number of breaches

[10] https://www.ixiacom.com/company/blog/benefits-cyber-range-training

grows steadily, with the incident response and attack defence techniques being time-critical, as the majority of compromises (87%) occurring within minutes[11]. This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks. Cyber Ranges (CR) are steadily gaining popularity as a means to prepare cyber security professionals and fill the industry's skills shortage. Although CRs have become quite sophisticated and support advanced attack features and scenarios, they exhibit the current business and technical hurdles:

- Focus on the network and application layers. Although the primary purpose of a CR is to facilitate the development of technical skills in cyber security, the learners often tend to neglect that a security incident is a business rather than a technical incident. Furthermore, CRs do not consider human factors and personal aspects. The benign activity simulation is mostly rudimentary and is based on macro recording and reproduction tools to simulate normal user activity, failing thus to capture the variety and wealth of user activities.
- Unbalanced datasets. The ratio of normal to attack traffic is typically low in CR environments. This leads to unconscious bias where an observable activity is tending to be malicious by default rather than the other way around. Moreover, malicious activity that is associated with outlier behaviour is not effectively simulated and as such the training is incomplete.
- Isolated incidents, with limited correlation history. In many cases the attack context is superficial, with the attacks being loosely correlated, failed attacks and lateral movements not being included or not represented accurately. The implementation of narratives based on kill chain type of approaches is limited. As such, current CRs do not allow the study and development of the challenging domain of cyber attribution.
- Limited duration. Due to resource constrains (both computational and personnel availability), the whole CR training experience is skewed as it is bound by the unrealistic short periods of activities. Such an arrangement for instance prohibits the investigation and detection of reconnaissance activities, through direct observation or OSINT exercises.

This paragraph depicts the key characteristics of major part of the existing cyber ranges and outlines some of the typical limitations, the following paragraph will introduce some concepts regarding future developments in this fields.

5. Developments: Further Developing Cyber Range Platforms

The present paragraph introduces the main concept of an innovative Cyber Range to be integrated in the foreseen European Cyber Range Network; it describes a platform devoted to easily create virtual environments dedicated to cyberwarfare training and cybertechnology development. Among the others, a potential roadmap to innovate cyber ranges will integrate, under a common platform, existing heterogeneous cyber security infrastructures and provide the means for expansion through a modular, scalable architecture. The cyber ranges will be interactive, simulated representations of an organization's local network, system, tools, and applications that are connected to a simulated Internet level environment. They will provide a safe, legal environment to gain hands-on cyber skills (based on a Cybersecurity Competence Based Curriculum) and a secure environment for product development and security posture testing. Thus, the foreseen architecture will be strongly linked with the NATO Multinational Cyber Defence Education and Training Project (MN CD E&T[12]). A cyber range will include actual hardware and software situated at the pilot sites or hosted in cloud environments and they

[11] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf
[12] http://mncdet.wixsite.com/mncdet-nato

will be a combination of actual and virtual components. Native nodes will be fully interoperable, and other CR environments will be partially interoperable forming the cyber range network, ECRN[13] tightly cooperating with cybersecurity coordination centres (e.g. CERTs/CSIRTs). At minimum, the level of integration will be through the Dashboard offering an overview of the different resources. In a more advanced level of integration, access to the assets and main components will be done by the APIs, whereas at the very end of the spectrum, complete integration will be offered on the network layer, concerning the CRs with SDN and NFV[14] capabilities, using standard management protocols such as OpenDaylight, and ONOS, allowing a high degree of control and efficient management of the network assets. The platform will connect different Cyber Ranges active in different environments and will consist of a variety of dynamic simulators with gamification capabilities that allow mechanisms for real time interactions and information sharing, as well as training and learning exercises based on a comprehensive cybersecurity competences model. In line with typical simulators' features, the platform will be capable of supporting real case studies and will create a knowledge base of cyber threats and related extended effects, as well as mitigation actions and countermeasures.

The solution is in line with typical simulator's features will be fed by real case study and will create a knowledge base of cyber treats and related extended effects and mitigation /counteractions. A specific feature is the identification of the zero-day vulnerabilities in order to reduce or eliminate the Window of Vulnerability (WoV) and identify main attack vectors. It provides a simulated environment to conduct tests and rerun exercises to enhance cyber defence technologies and skills of cyber defence professionals, in addition simulation features will offer a global situational awareness on the risk-chain and related attack surfaces. The proposed solution provides 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 cyberinfrastructures and IT systems used by government and private organisations. The platform enables 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 it will offer to cyber professionals the opportunity to develop the skills facing a relevant number of cyber-attacks and their overall impact. This 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 that can be scored even as economic savings, will receive suggestions on the best practice in the specific situation as identified by the platform or retrieved in the knowledge base.

The platform will:

- Provide performance-based learning and assessment;
- Provide a simulated environment and serious games where teams can work together to improve teamwork and team capabilities;
- Provide real-time feedback, for effective cyber risk management;
- Forecast new threats (plus their cascading effects), emerging attacks;
- Simulate on-the-job experiences;

[13] European Cyber Range Network

[14] Software-defined networking (SDN) and network function virtualization (NFV)

- Simulate a complex socio-technical environment in which people, procedures and technologies interact;
- Provide an environment where new ideas can be tested and teams can work to solve complex cyber problems;

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

6. Results

The proposed platform will provide a simulated environment to conduct tests and rerun exercises to enhance cyber defence technologies and skills of cyber defence professionals. In addition, simulation features will include a global situational awareness dashboard, informing the user about the risks and associated attack surfaces of the simulated organisation(s). It will provide a platform and a toolkit placeholder to develop and introduce tools to be used for testing the resilience of networked, socio-technical and cyber physical systems in general by exposing them to realistic nation-state cyber threats in a secure, sandboxed facility without dropping the need and experience of threat intelligence and communication. Innovation lies also on effectively monitor and prevent cyber-attacks by means of on-line textual content analysis (e.g. social media), supported by innovative deep semantic algorithms. Since most of potentially useful online contents relevant for online cyber-threats are not available in the Surface Web, it implements existing methodologies and solutions for online source identification, crawling and indexing, by making them efficient and effective for contents in the Deep Web and Dark Nets, with the expectation of inclusion of additional tools through the Cyber Range Network. The platform will enable the conduct force-on-force cyber games/exercises, and cyber capture the flag (CtF); it will provide an 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, it will offer cyber professionals the opportunity to develop the skills through facing a wide range of cyber-attacks and their overall impact. The proposed CRs will allow organizations to learn and practice with the latest techniques in cyber protection, practitioners to create and practically test different defence and incident response strategies in short time. Upon completion of a training session the practitioners, as already stated, will receive suggestions on relevant best practices in the specific situation, identified by the platform or retrieved in the knowledge base.

7. Business Benefits

The underlying concept to foster the development of a Culture of Cybersecurity could change substantially the “window of vulnerability” both in case of private users and organisations. The impact of a strong “Culture of cybersecurity” on business and economy is quite evident both as a direct and indirect effect. Citizens and organisations will increase the level of trust in cybertechnologies with positive effects both on safety and security in a widest sense. These effects will involve smart cities, transportations, commerce, government, etc. The idea to add an additional score to the cyber range exercise evaluation is due to the will to outline the business and economic savings due to a proper intervention.

8. Conclusions

We need to promote the awareness about cyber risks before the cyber technology will spread and control major part of reality, both adults and young generations must be aware

about potential risks. Some of the potential risks increase or reach a dangerous level as much as people use technologies disseminating personal information and content this implies that urges to inform users about similar risks sometimes not immediately evident. If security and safety will not be ensured a sentiment of unreliability may arose and delay the deployment of cyber technologies and e-services.

References

[1.] Weiser Mark D., The Computer for the 21st Century, Scientific American Ubicomp Paper after Sci Am editing, 09-91SCI AMER WEISER

[2.] Council of Europe (2001) New information technologies and the young. Council of Europe Publishing, Paris

[3.] Ronchi Alfredo M. (2019), e-Services: Toward a New Model of (Inter)active Community, Springer

[4.] Ronchi Alfredo M., The fourth screen, proceedings Global Forum 2010

[5.] Jones, Chris and Shao, Binhui (2011). The net generation and digital natives: implications for higher education. Higher Education Academy, York

[6.] Babel Chris, Tackling Privacy Concerns Is Key to Expanding the Internet of Things, Wired Innovation Insights, Feb 2015

[7.] Google - Privacy & Terms, https://www.google.com/intl/en/policies/privacy/

[8.] Burrus Daniel, Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/

[9.] Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic

[10.] Darrow Barb, The Question of Who Owns the Data Is About to Get a Lot Trickier, Fortune, http://fortune.com/2016/04/06/who-owns-the-data/

[11.] Mayer-Schönberger Viktor, Delete: The Virtue of Forgetting in the Digital Age, ISBN-13: 978-0691138619, Princeton University Press 2009

[12.] 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