Security, Safety, Defense,
Disaster Management and Recovery
Cluster del Politecnico di Milano

Issue no. 3 (2019): Defence Technology Foresight

Hybrid threats: defence line from the grassroots

Alfredo M. RONCHI
Chair JRC S2D2 - 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. The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario to reach the goals underpinning a conflict. A new type of hostile actions can be grouped under the umbrella of "hybrid threats", a mixture of coercive and subversive activity, conventional and unconventional methods. A pure cyber conflict is based on bit and bytes "soldiers" attacking key cyber assets ranging between markets and stock exchange to citizens' behaviour and "smart" objects. This new approach will enable state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. This term includes: massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats. Global networking is one of the building blocks of our society, communication, information, government, health, education, mobility, markets, the list of involved sectors is endless, all of them rely on cyber security and the trustfulness of the information provided through the network. An even increasing volume of information is flowing through the network including messages concerning potential future risks or cyber-weapons. There is a clear need to adopt a renovated set of countermeasures to face and possibly cancel or mitigate such harms. Big data analytics, artificial intelligence and machine learning together with other technologies may help in these tasks. Governments and Law Enforcement Agencies are aware of this and look for potential countermeasures not only following traditional solutions. Anyway technological countermeasures are not enough there is a need to foster the Culture of Cyber Security as a first defence line.

Keywords: Hybrid Threats, Cybersecurity, Culture of cybersecurity, ethics, privacy

Introduction

The paper entitled "21st Century cyber warfare[1]" provided a synthetic description of the discontinuity between the evolution of warfare as it was in a pre-cyber era and the switch to cyber warfare. The evolution from bronze to iron weapons, and later to gunpower weapons and flying objects does not compare with the cyber era warfare, even UAV and "intelligent" missiles

[1] Alfredo M. Ronchi, *21st Century cyber warfare*, Information & Security: An International Journal vol.39, 2018, Published by ProCon Ltd.

does not provide a significant understanding of the actual and near future scenarios. Following the fil-rouge that links together "wars" we find different typologies of weapons some of them forbidden by international treaties some usable, we find symmetric and asymmetric conflicts, guerrilla, terrorism and more. If we start considering the cyber warfare as something tightly connected with the traditional warfare as it might appear the use of drones and UAVs we risk to underestimate and depict an unrealistic scenario of cyber warfare. We need probably to reshape the definition of war or at last the definition of main wars, minor/local conflicts will probably continue to be fight by the force of conventional arms. A new type of hostile actions can be grouped under the umbrella of "hybrid threats" [1 - European Commission 2016], a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. This term includes: massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

Which is the aim of a future "war": to financially and economically dominate another country/ies, to reduce the competitiveness of a country? to incorporate new territories? to dominate strategic resources? to ensure a "New World Order"? to impose specific beliefs or life styles? the list may continue.

The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario to reach the goals underpinning a conflict [2 – European Union 2016]. The shift is between the scenario based on more or less traditional warfare "tools" like bombs, missiles, drones that are in danger because of the cyber part of their equipment and a pure cyber conflict [3 – European Union 2013] based on bit and bytes "soldiers" attacking key cyber assets ranging between markets and stock exchange to citizens' behaviour. Cyber technology is nowadays pervasive and utilised world-wide. Global networking is one of the building blocks of our society, communication, information, government, health, education, mobility, markets, the list of involved sectors is endless, all of them rely on cyber security and the trustfulness of the information provided through the network. An even increasing volume of information is flowing through the network including messages concerning potential future risks or cyber-weapons. There is a clear need to adopt a renovated set of countermeasures to face and possibly cancel or mitigate such harms [4- European Parliament 2019]. Big data analytics, artificial intelligence and machine learning together with other technologies may help in these tasks.

Setting the scene

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" [5 - Weiser 1991] phase, "users" are overlapping more and more with "citizens" [6 - Council of Europe 2001] and they consider technology and e-Services [7 – 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. Citizens, small, medium and big enterprises are more and more storing their data and information on clouds, procedures and production pipelines are more and more automated and robotized, products themselves are incorporating increasing portions of cyber technologies, software as a service approach is quickly gaining the stage. The more we become digitalised, the more we are vulnerable to hackers and hybrid threats.
Of course, the overall scenario includes many other aspects and "shades", this paper poses the focus on the "grassroots" of hybrid threats, citizens in their everyday use of cyber technology.

A diffuse "culture" of cyber security

The spread of cyber technology among citizens from kids to seniors together with the key role of such technologies both in accessing public and private services and performing everyday activities increases the risk of cyber-attacks aimed to ignite chaos and even injury citizens. We already faced a number of relevant attacks due to hackers, some targeting Governmental or Law Enforcement agencies and Institutions, some targeting critical infrastructure, some targeting big companies and even private cars and home appliances. Today's industrial machinery are fully computerised, PLC can be hacked both in factories and on board of aircrafts or other devices. Financial markets can be influenced or upset by cyber-attacks, critical infrastructure management can be jeopardised and the whole target infrastructure may collapse. Moreover, when cybersecurity strictly speaking is ensured it may be the human being the weak link in the chain. Furthermore, the key role of platforms and the fragility of the digital infrastructure and ecosystem do not mitigate the potential drawbacks.

If we simply refer to the Internet this infrastructure was created "weak by design" and the attempts to reshape it to make it secure didn't succeed yet[2]. The relevance of cyber infrastructure nowadays is outlined by the "undeclared" wars among cyber technology leaders. If in the recent past the control of the Internet was one of the key issues[3] – Who is going to rule the Internet? – today the quest for 5G[4] and artificial intelligence technology leadership is the hot topic even hotter than quantum computing leadership. 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 [8 - 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

[2] E.g. IP V6 protocol try to fix some aspects, Open Root initiative offering a second source against the unique Internet.
[3] Between 2003 and 2005 this was one of the hot topic partially solved with the Tunis Agenda and the creation of the Internet Governance Forum (IGF)
[4] Huawei 5G leadership - https://www.huawei.com/ca/industry-insights/innovation/5g-leadership

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 at affordable prices 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 [8 - 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!
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 [9 – Jones 2011], nowadays already on line[5].
Many times, in the ICT sector 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 that 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. This can be considered the first building block of a defence line against hybrid threats. 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 and more important counteract or mitigate the impact of a potential cyber war. This task is even more relevant than the efforts devoted to bridge the digital divide, the cultural divide is more critical. We must embrace a "culture" of cybersecurity starting from young generations, they risk to be victims of different types of criminal actions like cyber bulling, blackmails, extortions and in the future, they will be the defenders of our society.

Awareness, Education and Live Training

To contribute to bridge cybersecurity divide we can foresee a methodology based on 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 (January 2019)[6], a couple of workshops on the occasion of the WSIS Forum[7] (April 2019), and IST Africa[8] (May 2019).
The first action to be performed is to improve awareness about the potential risks due to improper use of digital technology both due to direct and indirect risks.

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

[5] It is a common understanding that recent generations 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].
[6] https://issuu.com/cyberfuture/docs/2019_cyber_future_dialogue_resoluti
[7] https://www.itu.int/net4/wsis/forum/2019/Home/Outcomes#documents
[8] http://www.ist-africa.org/Conference2019/

"fidelity cards" and the explosion of CRM[9]. 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[10]. This last aspect, "never disappear", takes us to another relevant point. Introducing the concept of data ownership, we make reference to the copyright concept. If my data are mine I can even delete them, isn't it?

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. Dealing with cyber warfare and hybrid threats potential breaches in security can be accomplished starting from privacy infringements. Breaches in personal data can open the doors to cyber-espionage. Cyber criminals are often forerunners in technological development and benefit from it, while measures for countering cybercrime are often one step behind.

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[11]" 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[12], 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 [10 – 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?" [11 - 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.

[9] Customer Relationship Management.
[10] We will not analyse the impact of GDPR on the above mentioned aspects in the present paper, refer to Ronchi, A.M., e-Citizens: Toward a New Model of (Inter)active Citizenry, ISBN 978-3-030-00746-1, Springer 2019
[11] Kind of neologism stressing the incredible proliferation of APPs.
[12] Typical example is "Fitness tracking app Strava gives away location of secret US army bases" https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Owning Information

As a direct consequence we will probably think about the concept of "ownership" of data and information. The concept of "data" as it relates to people's everyday life is still evolving [12 – Burrus 2014]. We inherited the concept of copyright and we more recently faced the concept of privacy [13 - 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 [14 – Darrow 2016].

Historically speaking, the idea of even owning information is relatively new[13]. The earliest copyright laws, which granted the creator of artworks, among the other rights, 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?

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. For our purposes the concept of "security" in the cyber world encompasses the whole universe from hacking to fake news. 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

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

anywhere anytime[14]. 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 and possible hybrid threats, such courses are now compulsory for both students, professors and public administration 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 (WSIS) devoted since 2005 a specific action line "Building confidence and security in the use of ICTs[15]" [15 – UN General Assembly].

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. 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. We must not forget that the weakest link of the security chain is usually the human factor.
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).

Technology may help: Live Training

Awareness and educational initiatives must be planned to provide a significant contribution to bridge the "cultural" gap but a live training is needed. Actually, the access to training infrastructure is mainly limited to big enterprises and governmental institutions principally due to the cost and complexity of such solutions we hope in the future it will be possible to find tailored solutions suitable for small enterprise and even citizens. Live training actions can be based on Cyber Ranges, a typical solution to train[16] and test cybersecurity measures and exercise professionals. 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 [16 – Council of the European Union 2018]. 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[17].

Some recent events may be summarized as follows: After the attack to Sony Pictures, to get closer in time, on the occasion of the 2016 Presidential elections there arose the suspicion of a potential mass intervention of foreign hackers influencing the results of the ballot.

[14] https://www.dejavusecurity.com/blog/2018/9/13/cybersecurity-and-video-games & https://www.researchgate.net/publication/222511796_A_video_game_for_cyber_security_training_and_awareness
[15] http://groups.itu.int/stocktaking/About/WSISActionLines/C5.Cybersecurity.aspx
[16] https://www.ixiacom.com/company/blog/benefits-cyber-range-training
[17] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

The progression of cyber-attacks is amazing; let's consider year 2017:

January 2017, the EU raises an alarm on fake news and hacking. EU commissioners have raised fresh concerns about fake news and hacking in Europe but warned that there are "no easy solutions".

February 2017, Yahoo sends out another round of notifications to users, warning some that their accounts may have been breached as recently as last year. The accounts were affected by a flaw in Yahoo's mail service that allowed an attacker—most likely a "state actor," according to Yahoo—to use a forged "cookie" created by software stolen from within Yahoo's internal systems to gain access to user accounts without a password. A number of other attacks include the so-called Zcoin; a simple one-digit typo within the source code of a cryptocurrency called Zcoin has allowed a hacker to make a profit of over $400,000 worth of cryptocurrency.

March 2017, UK: 26 million NHS patients' records in a security scare over SystmOne "enhanced data sharing"; "Privacy campaigners last night said the breach was "truly devastating" with millions of patients having no idea if their records had been compromised. GP leaders said the breach had "potentially huge implications" and could see family doctors flooded with complaints." (source "The Telegraph").

April 2017, Cyber Attacks Statistics, motivations behind the attacks: Cyber Crime 71,1%, Cyber Espionage 21,2%, Hacktivism 3.5%, Cyber Warfare 1.2% (source Hackmageddon). Scottrade Bank data breach exposes 20,000 customer records, 60 GB MSSQL database contained customer records and other sensitive data (source CSO from IDG).

http://www.hackmageddon.com/, last accessed 22 November 2017.

https://www.csoonline.com/article/3187480/security/scottrade-bank-data-breach-exposes-20000-customer-records.html, last access February 2018.

May 2017, ransomware WannaCry caused global chaos; Wired magazine titled it "The Biggest Cybersecurity Disasters of 2017 so far". The Guardian issued an article starting with the following sentences: "Massive ransomware cyber-attack hits nearly 100 countries around the world - More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA".

June 2017, a ransomware called Petya, which holds data hostage by scrambling it until a payment is made, caused widespread disruption across Europe and the United States.

July 2017, Italy, UniCredit bank was attacked by hackers; they have taken 400,000 IDs, but apparently no code or password that allows them to operate without authorization on current accounts. July 2017, Reuters - Cyber attackers are regularly trying to attack data networks connected to critical national infrastructure systems around Europe, according to current and former European government sources with knowledge of the issue.

August 2017, Russian hackers are targeting hotels across Europe; the hackers used booby-trapped Word documents and a leaked NSA hacking tool to get a foothold into the networks to then attack guests.

September 2017, The Guardian alerts: Hackers attacking US and European energy firms could sabotage power grids, water, gas; and a joint report presents physical and network-based malware affecting ATMs. September 2017, online sexual extortion: man sentenced in Romania in connection with death of British teenager.

September 2017, European Union Agency for Network and Information Security, ENISA, inaugurated as permanent EU cyber security agency. Europol's European Cybercrime Centre (EC3) and Trend Micro, a global leader in cybersecurity solutions, and released a comprehensive report on the current state of ATM Malware.

October 2017, the internet of things: when your washing machine and blood pressure monitor become a target for cyberattacks. October 2017, 195 individuals detained as a result of global crackdown on airline ticket fraud.

November 2017, British cryptocurrency Electroneum hit by cyber- attack after raising £30m, the cyber-attack that has shut investors out of their accounts for several days. The company's website came under a distributed denial of service (DDoS) cyber-attack. Similar attacks to South Korean cryptocurrency.

This short summary of attacks covering almost one year looks like a war report; the increasing pace of new attacks is amplified by the almost daily creation of new segments of cyber services and technologies. 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.

The cyber ranges are interactive, provide a 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, this architecture is strongly linked with the NATO Multinational Cyber Defence Education and Training Project (MN CD E&T[18]). 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. CRs 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 government and private organisations. They 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 it will offer to cyber professionals the opportunity to develop the skills facing a relevant number of cyber-attacks and their overall impact.

Similar platforms 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 may include a global situational awareness dashboard, informing the user about the risks and associated attack surfaces of the simulated organisation(s). These platforms will provide 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 specific ontologies, on-line textual content analysis (e.g. social media), supported by innovative deep semantic algorithms and machine learning tools. Since most of potentially useful online contents relevant for online cyber-threats are not available in the Surface Web, the CR platform 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 a Cyber Range Network. These platforms will enable the conduct force-on-force cyber games/exercises, and cyber capture the flag (CtF); they will provide an environment to integrate technologies and test company-wide cyber capabilities,

[18] http://mncdet.wixsite.com/mncdet-nato

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, they will offer cyber professionals the opportunity to develop the skills through facing a wide range of cyber-attacks and their overall impact. These platforms 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 will receive suggestions on relevant best practices in the specific situation, identified by the platform or retrieved in the knowledge base.

Benefits due to a "Culture of Cyber Security"

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 cyber technologies with positive effects both on safety and security in a widest sense. These effects will involve smart cities, transportations, commerce, government, etc.

Conclusions

To improve resilience and mitigate risks due to hybrid threats we need to promote 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 but potentially dangerous even in case of hybrid threats. If security and safety will not be ensured a sentiment of unreliability may arose and delay the deployment of cyber technologies and e-services. This will be the first defence line at grassroots level of course more specific and sophisticated actions will complete the overall defence schema.

References

[1.] Joint Framework on countering hybrid threats a European Union response, European Commission JOIN(2016) 18 final, 2016
[2.] Shared Vision, Common Action: A stronger Europe, European Union, June 2016
[3.] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final
[4.] European Defence Action Plan: Towards a More Competitive and Efficient Defence and Security Sector, European Parliament Legislative Train 04.2019
[5.] Weiser Mark D., The Computer for the 21st Century, Scientific American Ubicomp Paper after Sci Am editing, 09-91SCI AMER WEISER
[6.] Council of Europe (2001) New information technologies and the young. Council of Europe Publishing, Paris
[7.] Ronchi Alfredo M. (2019), e-Services: Toward a New Model of (Inter)active Community, Springer
[8.] Ronchi Alfredo M., The fourth screen, proceedings Global Forum 2010
[9.] Jones, Chris and Shao, Binhui (2011). The net generation and digital natives: implications for higher education. Higher Education Academy, York

[10.] Babel Chris, Tackling Privacy Concerns Is Key to Expanding the Internet of Things, Wired Innovation Insights, Feb 2015
[11.] Google - Privacy & Terms, https://www.google.com/intl/en/policies/privacy/
[12.] Burrus Daniel, Who Owns Your Data?, https://www.wired.com/insights/2014/02/owns-data/
[13.] Merriam Webster: Ethic, http://www.merriam-webster.com/dictionary/ethic
[14.] 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/
[15.] 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
[16.] EU Cyber Defence Policy Framework (2018 update), Council of the European Union 2018