S2D2
Security, Safety, Defense,
Disaster Management and Recovery
Cluster del Politecnico di Milano

INTERNATIONAL CONFERENCE ON ‘HOMELAND’ SECURITY:
Emerging Trends, Challenging Aspects

Panel III. Homeland Security for Soft Concerns: Expanding the Context

“Soft” but still concerns

Alfredo M. Ronchi
JRC S2D2 – Politecnico di Milano
alfredo.ronchi@polimi.it

Abstract

Starting from the switch from institutionalized state to the concept of homeland and related security measures and initiatives the paper will focus on soft concerns like illegal immigration, uprisings, terrorism, pandemic diseases, natural disasters, misuse of cyber space, economic speculations etc. Soft concerns potential impact and possible counter measures or mitigation actions. Both citizens perception of homeland and potential security risks evolved in recent times, globalization and on-line communication had a deep influence on citizens' perceptions and lifestyle. 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. A kind of butterfly effect that propagates in real-time from continent to continent. So, if one of the key enablers of soft concerns is cyber technology this is even one of the most relevant countermeasures.

This paper provides a synthetic description of the discontinuity between the evolution of warfare as it was in a pre-cyber era and the switch to the different levels of cyber “warfare”. There is a clear need to adopt a renovated set of countermeasures to face and possibly cancel or mitigate new threats.

Introduction

Through time the concept of safety and security evolved from the freedom from danger to be hurt by wild animals to airline improved protection against failures, from measures taken to guard against enemy tribe attacks to freedom from the prospect of being laid off.

Once upon a time key security issues at national level were concentrated on enemy states, hard power was the counter measure, nations use to challenge facing respective hard power. The evolution of potential threats forced to re-shape the “enemy” from countries to groups and individuals challenging with a wide range of “weapons” on different domains: digital, economic, healthiness and more the wideness of the range of challenges forces to redefine the institutional definition of state to a more effective concept of homeland, this improve the sense of belonging to a common fate. The concept of homeland security enforces the idea of 360-degree security whatever is the threat.

Total Security or Different Levels of Insecurity?

Posing the focus on security nowadays we usually consider “security” as a seamless part of our life, apparently something cost-free, no need to invest or care about it. This seems to be true till we face minor or big problems. Pickpockets take our wallet, thief stole our car or take some of the goods we have at home, hackers kidnap our data. Therefore, we start to be concerned about security, it is no more a cost-free “commodity”, we need to invest some resources to reach “a certain level of "insecurity" quoting Salman Rushdie. Why we say "level of insecurity"? Because generally speaking there is not total security or better "There is no such thing as perfect security, only varying levels of insecurity." We will come back on this concept later in this paper.

As the general concept of security evolved through time the concept of national security evolved as well and, the same happened in case of potential targets and threats. State actors face a very complicated scenario trying to match with the current and future developments of threats based on risk assessment, probability and projections. Many times, in this complex and risky scenario, the best or less harmful solution is to refer to the game theory and how to maximise the gain minimizing risks. This may led to choices motivated by contradicting goals.

National Security

The evolution of national security in recent times extended the spectrum of potential threats actors to individual human, social groups, non-state actors either armed or not. So, threat conceptualization has changed it includes massive migration, single or organised terroristic groups, and other non-state actors; simply consider the perceived environmental and humanity security under the shade of climate change.

Potential countermeasures deal with prevention of potential attacks and mitigation of possible impact because soft targets usually lack capacity to strike back against attackers. If we refer to terroristic groups or single activists they do not have "homeland" to strike back, the same in case of hackers and cyber-attacks. Key actors of such measures belong to governmental bodies, communities or less frequently from private subjects.

So, homeland security unified under a unique dome all the security measures including completely new ones like "triangulations" or 'pre-emptive measures' like "pre-emptive war" as it happened mainly in the USA. This paper will focus on a specific subset of threats the "soft concerns" and the role of cyber technologies in this domain.

Soft Concerns

The evolution of threats and related security conceptualisation comprise both hard and soft concerns. Nation state hard power is represented by the army supported by its own intelligence, this is not one hundred per cent suitable or enough in case of soft concerns. The protection of soft targets is usually a domain governed by the Ministry of Interior, while the Ministry of Defence is usually in charge for hard warfare.

Nowadays we face 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". To build a sounding information society we must efficiently counteract cyber-criminality and establish a clear vision on legal behaviours in the cyber-world.

The key challenge is to determine what the drivers of new forms of cyber criminality are and how they might be prevented and mitigated. There is a clear need to adopt a renovated set of countermeasures to face and possibly cancel or mitigate such harms. This comprehensive approach requires a strong interdisciplinary methodology ensuring a tight interaction among human factors experts, sociologist, psychologists, cyber-psychologists, anthropologists, technologists and experts in organisational aspects together with lawyer, law enforcement agencies and practitioners. Thanks to this broad inter and cross disciplinary team, different skills and way of thinking will continuously collide to ensure critical thinking, the inclusion of some “divergent-thinker” will favour out of the box solutions.

Transnational terroristic organisation many times do not have their homeland to be attacked by regular army, individual if properly trained can cause relevant damages. One of the definitions of soft-threats is “Soft threats usually refer to security that protects something from harm in quiet and unobtrusive ways, often invisibly and after the fact, rather than with visible barriers before the fact”. This is the domain of soft concerns like illegal immigration, pandemic diseases, natural and human disasters, cyber space threats, hybrid threats, economic speculations and more.

Illegal migration represents a relevant concern in different areas of the world from United States to Africa and Mediterranean countries. Sometimes migrants are moving autonomously, many times criminal organisations are key player in the sector. A proper network of observers reporting the potential risk of migration from a specific area toward a country or region is one of the basic measures on the field. In addition to information services and intelligence cyber technology provides valid tools and technologies to identify and trace migration, remote sensing, satellites, drones as well as information flow analytics.

Large amounts of data and information from a variety of origins have become available to practitioners involved in fighting crime and terrorism. Full advantage is not currently taken of the most advanced techniques for Big Data analysis, and artificial intelligence and machine learning. The amount of data flowing through the network is increasing every day at exponential pace. Data are geo time-series, raw data, social media and media analytics, open source intelligence, socio-economic and geo-political factors, human factors, potential influencers, feedbacks to specific solicitations, crowd sourcing, remote sensing. When faced with massive and heterogenous streams of data, however, an effective means of synthesising, extracting and reporting relevant data to law enforcement authorities (LEAs) proves a major challenge. Effectively meeting this challenge depends on state-of-the-art knowledge of cybercrime and terrorism, including its expected developments, trends and ways of preventing and countering it, as well as technical expertise to design and implement technology that draws on and efficiently presents anomalies found in many different data sources. A proper knowledge and use of state-of-the-art technologies can provide a relevant support to fight against (cyber) crime and terrorism. If on one side technologies can offer new opportunities to criminals on the other side they, if properly used, can offer a significative help to law enforcement agencies both in the prevention, mitigation and neutralisation.

Cyber Attacks

The increasing role of cyber technology in our everyday life and key services increases at the same time and even more the risk of cyber-attacks. We already faced a number of relevant attacks due to hackers, some targeting Governmental or Law Enforcement agencies and Institutions, some targeting critical infrastructure, others targeting big companies.

Financial markets may be influenced or tilted by cyber-attacks. Smart cities and grid models must carefully consider cyber security issues; we don’t appreciate the “rebellion” of elevators or the unwanted locking of all the entrance doors of our company headquarters. As much as we install IoT and other cyber devices and services as much the risk to be cyber-attacked increases.

What about industrial machinery today fully computerised, or critical infrastructure management; in a cyber warfare scenario it might be enough to dispatch on the network a code name like “1024 millibar” to collapse the whole target infrastructure[1].

Today even cars may be subject to cyber-attacks as it already happened to Jeep cars[2] in the United States; if on one side the regular car service or recall for update can be performed through the permanent car connection to the Internet, no more requiring to physically take the car to be serviced, on the other side, in case of cyber-attacks, our car might behave in an unpredictable way. This to do not mention aircrafts, ships, trains, metro and any other transportation means, PLC and more in general software programs are easily hacked, this even because they were designed in and for a hacking free environment. We are surrounded by “critical infrastructures” that, in case of attacks, may create mayor or minor impact on our daily life. We don’t mean only typical critical infrastructures like communication, energy, water, health, transportation, and last but not less important nowadays financial services; we consider information services, social media, geo-positioning, home automation, smart cities, safety and security devices, and more.

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, as it happens in case of social engineering.

Typical examples of massive cyber-attacks were WannaCry, Petya that we all know. Through 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.

Similar situations recall the concept of different levels of insecurity, due to lack of investments in cyber security, from personal devices to big companies, the risk to face a cyber disaster is always active. Proper use of risk assessment procedures and related mitigation plans use to enforce the so called “cyber resilience” safeguarding business continuity, suffering the minimum possible damage.

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, CSIRTs and CERTs, cyber ranges exercises, key personnel specific training 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, Secretary Ministry 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.

[1] This to do not mention Wanna Cry and the registered domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

[2] This was in reality a demonstration to outline the potential threats due to pervasive use of digital technology in the automotive sector.

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, this encompasses a proper risk analysis and awareness.

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 all the potential dangers or attacks. Once we have a list of specific vulnerabilities for each "critical 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, potential intrusions, human factors, etc). to map the overall risk. This methodology usually involves a clear understanding of all the potential interrelation both between "nodes" and dangers, the identification of the single and overall risk is usually determined thank to an analytical method such as Bayesian networks. This methodology provides the opportunity to perform a valuable risk analysis and prepare countermeasures or mitigation actions. 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 communication 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, of course, was to ensure as much as possible business and education 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[3], 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 cyber-sovereignty 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.

[3] This not considering citizens locked down at home watching movies and playing music in digital streaming.

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.

Privacy infringements: risk assessment mapping

As already stated, we all know that security and privacy are subject to risks; 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 subject at risk in the event of sensitive 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:

1) Digital information security;
2) Physical and operational security;
3) 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).

Cyber Sovereignty

While cyber sovereignty is a vague concept in general that is often used in relation to state power and independence in cyberspace, sovereignty itself is a clearly defined concept in International Law. Therefore, the concept of cyber sovereignty needs to be defined more precisely. Nowadays the principle of sovereignty is paramount. The sovereignty of the state forms the fundamental basis of the current international Law and order trace back in 1648. The Peace of Westphalia, signed to end the thirty years war, established the Westphalian system of considering states to have sovereignty over their respective territories and domestic affairs, in which other states should not interfere (Franzese 2009).
As outlined above the concept of cyber sovereignty is vague, one of the possible definition due to Baezner and Robin is: “the application of principles of state sovereignty to cyberspace” (Baezner and Robin, 2018). Another definition should be “the possibility for users to have control over their own data” but this definition lacks the element of state control over data (De Filippi and McCarthy, 2012).

Traditional concepts of state boundaries and the principles of International Law are challenged by the development of technology and cyberspace. Internet, in its early days was governed by its users[4] and considered to be immune to sovereignty due to its interconnectedness and transnational nature (Franzese, 2009), even if the architecture of the network was already managed by centralised authorities. Nevertheless, it was assumed that Governments would kept distance from Internet governance, the unprecedent power to reach mass audience and freedom of speech supported this idea. The increasing power assigned to the Internet and its potential applications in the military and governmental services as well as other relevant ones made the difference so, state involvement in the development of cyberspace become inevitable, this was more than clear once technology assumed a potential role in political gain. International discussions of the extent and applicability of state sovereignty to cyberspace came to replace the more idealistic views of the earlier era.

The shift to cloud computing and internet-based platforms become a standard for state departments; documents, data and messages were delivered through the network. A turning point that heightened international fears was 2013, due to Edward Snowden's revelations about the US Internet mass surveillance program. This data security breach imposed the redefinition of data protection policies for data generated and transiting over national territories. These actions strengthened the concept of cyber sovereignty so some economic actors have demanded greater cyber sovereignty to protect industrial and other economic sectors considering cyber sovereignty a form of autonomy in cyberspace.

This short overview showcase that the concept of cyber sovereignty is still misunderstood or distorted from its definition in International Law, so, it is interesting to consider the ways in which national states employ the concepts of sovereignty and cyber sovereignty in their national cybersecurity strategies. The approach to defining cyber sovereignty - in terms of state control and independence in cyberspace - is a controversial one, as it may conflate issues of strategic autonomy with the separate concept of cyber sovereignty.
The use of the concepts of sovereignty and cyber sovereignty in national cybersecurity strategies reveals that only a minority of states used the term "sovereignty", and only one used the term "cyber sovereignty". The concept was primarily used by Western states, referring to a definition of sovereignty that closely matched the understanding described by International Law. States' cybersecurity strategies mostly displayed awareness that cyberattacks may constitute a threat to state sovereignty, or to re-emphasize that state sovereignty should be protected. To achieve this end, states planned to improve cybersecurity in the information technologies and networks of governmental, defence and critical infrastructures. Among other European countries France as an exception; Paris referenced sovereignty most extensively throughout its national cybersecurity strategies emphasizing strategic autonomy over traditional sovereignty. Where strategic autonomy means a wider protection of state sovereignty, states maintains full control over data processing, data storage, and information technology infrastructures. Following this definition of strategic autonomy, this is no more equivalent to the concept of sovereignty.

United Nations cyber sovereignty

The United Nations Governmental Group of Experts [1] (UNGGE)[2] decided that International Law, including state sovereignty, was applicable in cyberspace (United Nations General Assembly,

[4] World Wide Web conference up to 2005 were the occasions to share ideas and showcase web advances

2015). This decision implied that the Law of Armed Conflict was applicable in cyberspace, as well as all rights and obligations tied to principles of sovereignty. The Tallinn Manual on the International Law Applicable to Cyber Warfare and the Tallinn Manual 2.0, which discuss the status of the current International Law in reference to cyberspace, came to the same conclusion regarding state sovereignty in cyberspace (Schmitt and NATO Cooperative Cyber Defence Centre of Excellence, 2017, 2013).

Researchers have outlined the physical dimension of sovereignty in cyberspace; physical infrastructures are necessary for the proper function of cyberspace, and most of those infrastructures are located on claimed territory, this apart from satellite and other space-based infrastructure regulated by specific law, these “objects” once target of “space-wars”. State sovereignty in cyberspace could therefore be seen as an extension of a state’s territorial sovereignty; of course, this logically includes the use of force in cyberspace or the right to use cyber-tools in war.

Data sovereignty - The concept of data sovereignty lacks a fixed definition but has been regularly used in politics, industries and law. We define data sovereignty as a state’s ability to control data originating and passing through their territory. The term data sovereignty was not used in national strategies, but may be discussed at other political levels. Edward Snowden’s revelations on the National Security Agency's (NSA) PRISM program US mass surveillance of the Internet. In response to Snowden’s revelations and states’ growing concerns over data management by cloud computing services offered by key players, numerous states developed regulations to supervise the use of data stored or collected by third parties. The European Commission, updating and extending previous regulations[5] , in 2016[6] issued a data protection Directive [25 Protection - EU], the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation entered into force on 24 May 2016, it applied from 25 May 2018. The Directive entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018. One of the improvements is the geographic coverage of the Directive, formerly one of the main critical aspects in both the national and international regulatory frameworks. The new regulation will apply if the data controller or processor (organization) or the data subject (person) is based in the EU. Furthermore (and unlike the previous Directive) the Regulation will also apply to organizations based outside the European Union if they process personal data of EU residents. This regulation, the GDPR, incorporates the French definition of Cyber Sovereignty. An additional interesting aspect is represented by the definition of “personal data”. According to the European Commission, "personal data” is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, “posts” on social networking websites, medical information, or a computer’s IP address. This is a relevant step forward in privacy issues

Hybrid Threats

As a side effect of globalisation and massive cyber services the number of crimes both perpetrated at local and global level is growing up. Cyber technology and its pervasiveness

[5] Directive 2002/58/EE of the European Parliament and of the Council of 12 July 2002 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML , last access December 2017.

[6] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, entered into force on 24 May 2016.

created a completely new scenario, the new type of hostile actions can be grouped under the umbrella of "hybrid threats" [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. "Hybrid threats" include: 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. As already stated above, 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. So, till what extent we are willing to give up our privacy to increase security? Which is the golden balance between privacy and security issues? 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.

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. 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[7]. 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[8] – Who is going to rule the Internet? – today the quest for 5G[9] and artificial intelligence technology leadership is the hot topic even hotter than quantum computing leadership.
In a society everyday more dependent from cyber technology there is a clear need to improve awareness about potential risks in the cyber universe. 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. To contribute to bridge cybersecurity divide we can foresee a methodology based on awareness, education and live training. 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

[7] E.g. IP V6 protocol try to fix some aspects, Open Root initiative offering a second source against the unique Internet.
[8] 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)
[9] Huawei 5G leadership - https://www.huawei.com/ca/industry-insights/innovation/5g-leadership

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. 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 digital transition phase ensure proper education to citizens. 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.

Cyber warfare

If we start considering the cyber warfare as something tightly connected with the traditional warfare as it might appear the use of drones, UAVs and UGVs 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. 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.

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.

The discontinuity ignited by cyber technology and the pervasiveness of this technology created the fundamentals for a completely new scenario to reach the goals underpinning a conflict [European Union 2016]. The shift is between the scenario based on more or less traditional warfare "tools" like drones, rockets, bombs that are in danger because of the cyber part of their equipment and a pure cyber conflict based on bit and bytes "soldiers" attacking key cyber assets ranging between markets and stock exchange to citizens' behaviour.

Human factors are of course deeply in the loop, social media can play a relevant role in shaping the public opinion nowadays much more that press and television. They can elicit the will to change the government, to feel oppressed or damaged by other countries, to join a different country because of economy, culture, etc….

Aircrafts both civil and military can be neutralised hacking them both on the ground or flying, no more need to be on board to hijack a flight or crash it, something like a smart phone will be enough.

As already outlined, Internet of things and networks of Sensors can be easily hacked providing useful information to cyber criminals. PLC can be hacked causing serious problems to factories, industrial plants and cyber controlled devices in general.

To mitigate the unconscious use of cyber technologies and the broad dissemination of sensitive data both at personal and organisation level there is a clear need to improve awareness education and training in cyber technologies starting from schools.

Among the other potential approached we will focus on two well-known families of systems: cyber ranges to test, train and simulate attacks and information and data stream analysis to intercept potential threats.

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, sand boxes, 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[10]". 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[11] released in 2013.

Later on, in 2017 the Communication "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU[12]" 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[13] 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[14]), which started operations in January 2013. EC3 is part of Europol[15] 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."

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[16] 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

[10] http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_ conv_budapest_en.pdf, last accessed January 2019.

[11] http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf or http:// eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri1⁄4CELEX:52013JC0001&from1⁄4EN, last accessed January 2019.

[12] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri1⁄4CELEX:52017JC0450&from1⁄4EN, last accessed January 2019.

[13] Simply consider digital preservation aspects.

[14] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3, last accessed January 2019.

[15] https://www.europol.europa.eu, last accessed January 2019.

[16] Pavan Duggal (https://www.itu.int/net4/wsis/forum/2016/Content/AgendaFiles/document/ 84895151-aeee-4a7f-a2f9-26bf03dc4bcf/A_BRIEF_PROFILE_OF_PAVAN_DUGGAL_(CS). pdf), Advocate at the Supreme Court of India, wrote more than 80 books on Cyber Laws and Cyber Crimes; he is Chair of Cyberlaws.net and chair of the International Conference on Cyber Law, Cyber Crime & Cyber Security, http://cyberlawcybercrime.com, last accessed January 2019.

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[17]". 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. 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.

The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations[18], 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[19].

Conclusion

To conclude let's recap the key points outlined within this paper, the concept of state and national security evolved in the concept of homeland and homeland security, cyber technology is nowadays pervasive and at different level present all-over the globe, digital data creation in

[17] http://meity.gov.in/writereaddata/files/HOW_TERRITORY.pdf, last accessed January 2019.

[18] ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html, last accessed January 2019.

[19] https://ccdcoe.org

the different formats are growing exponentially, tightening the relation between cyber technology, our everyday life, cyber sovereignty and homeland security. A number of potential risks can jeopardise our everyday life both due to human and natural causes: natural disasters, pandemic, human threats, hybrid threats, up to cyber warfare. Proper awareness and overall risk analysis together with the implementation of a "culture" of security extended from kids to seniors is required.

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. If security and safety will not be ensured a sentiment of unreliability may arose and delay the deployment of cyber technologies and e-services.

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. 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 a 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 threat scenario, the soft threat scenario, in which one single man located anywhere can create relevant damages globally. Citizens will be the first defence line at grassroots level of course more specific and sophisticated actions will complete the overall defence schema.

Bibliography

1) Babel C (2015) Tackling privacy concerns is key to expanding the internet of things, Wired Innovation Insights, Feb 2015
2) Baezner, M., Robin, P., 2018. Trend Analysis: Cyber Sovereignty. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/314398/Cyber-Reports-2018-01.pdf?sequence=1&isAllowed=y
3) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013) 1 final
4) 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

5) Damico Tony M (2009) A brief history of cryptography. Inq J 1(11): 1/1, 2015 Student Pulse. All rights reserved. ISSN: 2153-5760
6) Diffie W, Hellman ME (1976) New directions in cryptography. IEEE Trans Inf Theory 22 (6):644–654
7) Duggal P (2018) Cyber Law 3.0, LexisNexis, Gurgaon, India, ISBN 978-81-3125-366-3
8) European Commission (2017) Resilience, Deterrence and Defence: building strong cyber-security for the EU, JOIN (2017) 450 final
9) EU Cyber Defence Policy Framework (2018 update), Council of the European Union 2018
10) European Defence Action Plan: Towards a More Competitive and Efficient Defence and Security Sector, European Parliament Legislative Train 04.2019
11) 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
12) 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
13) Franzese, P.W., 2009. Sovereignty in Cyberspace: Can it exist? Air Force Law Review 64, 1–42. https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist
14) 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
15) Kahn D (1997) The Codebreakers: the story of secret writing. Scribner, New York. ISBN:978- 1-439-10355-5
16) Irion, K., 2012. Government Cloud Computing and National Data Sovereignty: Government Cloud Computing and National Data Sovereignty. Policy & Internet 4, 40–71. https://doi.org/10.1002/poi3.10
17) Joint Framework on countering hybrid threats a European Union response, European Commission JOIN(2016) 18 final, 2016
18) Jones, Chris and Shao, Binhui (2011). The net generation and digital natives: implications for higher education. Higher Education Academy, York
19) Milanov E (2009) The RSA algorithm, accelerated (honors) advanced calculus. University of Washington, Seattle
20) NATO Cooperative Cyber Defence Centre of Excellence (2017) Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press
21) Ompall, Pandey T, Alam B (2017) How to report cyber crimes in Indian territory. Int J Sci Technol Manag 6(04), April 2017, ISSN 2394-1537
22) 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
23) Peterson, Z.N.J., Gondree, M., Beverly, R., 2011. A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud, in: Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing. Presented at the HotCloud'11, USENIX Association, Berkeley, CA, USA, p. 5. https://www.usenix.org/legacy/event/hotcloud11/tech/final_files/Peterson.pdf
24) Polatin-Reuben, D., Wright, J., 2014. An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. USENIX Association.
25) Ronchi Alfredo M., (2019), e-Citizens: Toward a New Model of (Inter)active Citizenry , ISBN 978-3-030-00746-1, Springer (D)
26) 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

27) Ronchi Alfredo M., Duggal P et al, WSIS Forum 2016 Outcomes. https://www.itu.int/net4/wsis/forum/ 2016/Outcomes/

28) Ronchi Alfredo M., (2019), e-Democracy: Toward a New Model of (Inter)active Society, ISBN 978-3-030-01596-1, Springer (D)

29) Ronchi Alfredo M., (2019), e-Services: Toward a New Model of (Inter)active Community, ISBN 978-3-030-01842-9, Springer (D)

30) 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

31) Ronchi Alfredo M., (2018), 21ST Century Cyber Warfare, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018

32) Ronchi Alfredo M., (2018),, TAS: Trust Assessment System, in International Journal of Information Security, vol.39, ISSN: 1615-5262, Springer Verlag, 2018

33) Ronchi Alfredo M., (2018), Hybrid treats: defence line from the grassroots, NATO STO Issue no. 3: Defence Technology Foresight, Bulgarian Defence Institute, 2 Prf. Tsvetan Lazarov blvd. Sofia, Bulgaria

34) Ronchi Alfredo M., (2018), . . .1984 won't be like "1984"?, ISBN 978-5-91515-068-9, Interregional Library Cooperation Centre, Moscow

35) 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)

36) Shared Vision, Common Action: A stronger Europe, European Union, June 2016

37) SAS report on The Internet of Things. http://www.sas.com/it_it/offers/ebook/iot-visualise-the-impact/index.html

38) Thawte (2013) History of cryptography, an easy to understand history of cryptography. Thawte

39) 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

40) UNESCO (2014) Human development report 2014. Sustaining human progress: reducing vulnerabilities and building resilience

41) Virgo – Safety device for the protection of operators working in risky environment. http://www.intellitronika.com/virgo/