The Key Role of Interdisciplinary Communication in Cyber Security

Mario LAMANNA, Evoelectronics, Italy

WMSCI 2016

The 20th World Multi-Conference on
Systemics, Cybernetics and Informatics: WMSCI 2016

July 5 - 8, 2016 – Orlando, Florida, USA

CYBER SECURITY of Critical Infrastructures is one of the Third Millennium challenges

Secure Communications

Border Control

Electricity, Water, Gas, Oil Plant Protection

Transport Protection

Territory Protection

A Common Interdisciplinary Approach

Developments in electronics and computers during the last 70 years have created the so called Information Age.

A basic understanding of the Information Age, considering both technological and social aspects, is essential to consider cyber security issues.

The Information Age has transformed an economy based on industrial mass production to a new economy based on knowledge and control of information .

The development of knowledge and information is a product of a cumulative human endeavor, which represent multifaceted aspects of human life.

The main characteristics of the Cyberspace

The Cyberspace is the set of all computerized networks, end points, communication networks and computer based systems.

The knowledge is the most important element of the Cyberspace

The structure and design of the Cyberspace has a decisive influence on Cyber Security.

The Cyberspace with respect to Cyber Security

Rapid change in tools, including defense systems. Difficulty in tracking objects and finding sources of possible attacks.

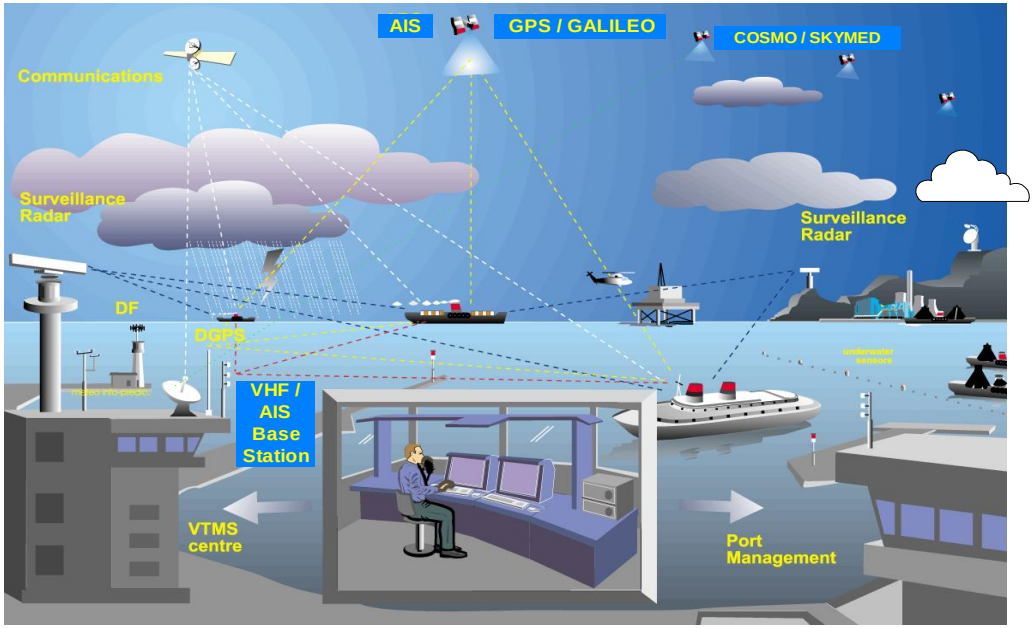
High level of complexity and consequent problems in distinguishing attacks from malfunctions.

High level of vulnerability of hardware and operating systems, due to the high volume of standard commercial on the shelf equipment used.

Relative low cost of cyber tools to prepare cyber attacks.

Lack of a clear legal environment, which encourages hacker actions and favoures some type of instability.

Cyber Security for Critical Infrastructures

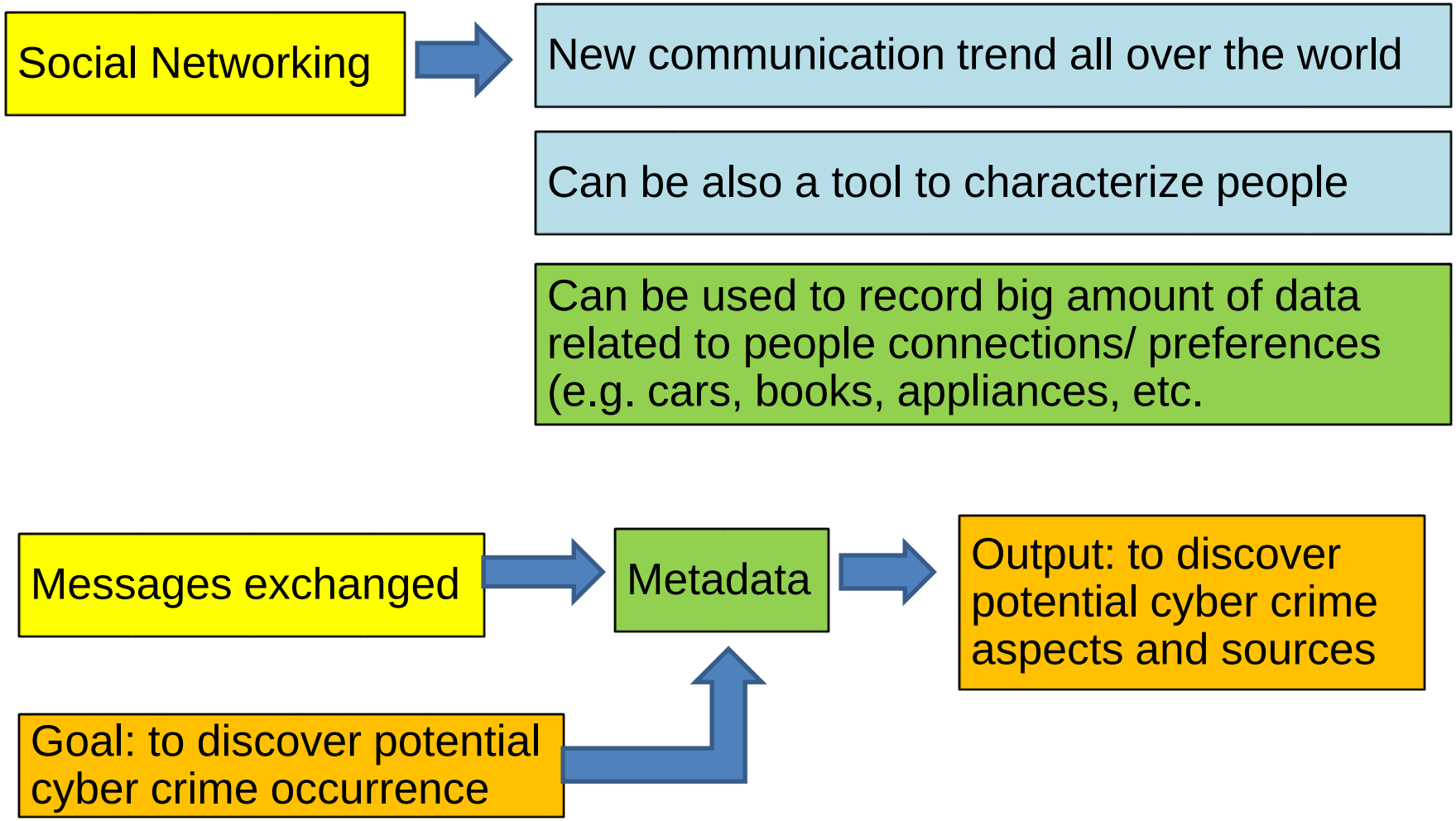


Cyber attacks against critical infrastructures can paralyze their activities or steal sensible information.

The consequence of a cyber attack can be disastrous, due to the essential services they perform.

There is a urgent need to find new effective solutions to enforce cyber security for critical infrastructures at maximum levels.

A Common Interdisciplinary Approach



Involved Technologies

Big Data

Intelligence

Deep Learning

Data Fusion

Human in the Loop

Big Data

Big Data represents the information assets characterized by high volume, velocity and quality, so that a specific technology and management methods are required to transform these data into information to be used by real applications.

The typical architecture used to process Big Data is based on the MapReduce concept, which consists of processing in parallel (Map) the data previously distributed across parallel nodes (Reduce).

Intelligence

Intelligence consists of a set of processes aimed to collecting, processing and interpreting information and knowledge relative to an adversary element (person/ organization), with the goal to activate defense actions against possible attacks from that element. As these processes are mainly based on brain power and experience, intelligence is typically referred to human beings, but at least part of the processes can be automated and performed by machines (e.g. artificial intelligence tools).

Deep Learning

Deep Learning is a branch of machine learning, consisting of a set of algorithms, which model non linear data transformation by using multiple processing layers. At each layer, data are transformed by a processing unit, like an artificial neuron, whose parameters are learned through training. The overall structure of a deep learning network is inspired by a biological model of the human brain.

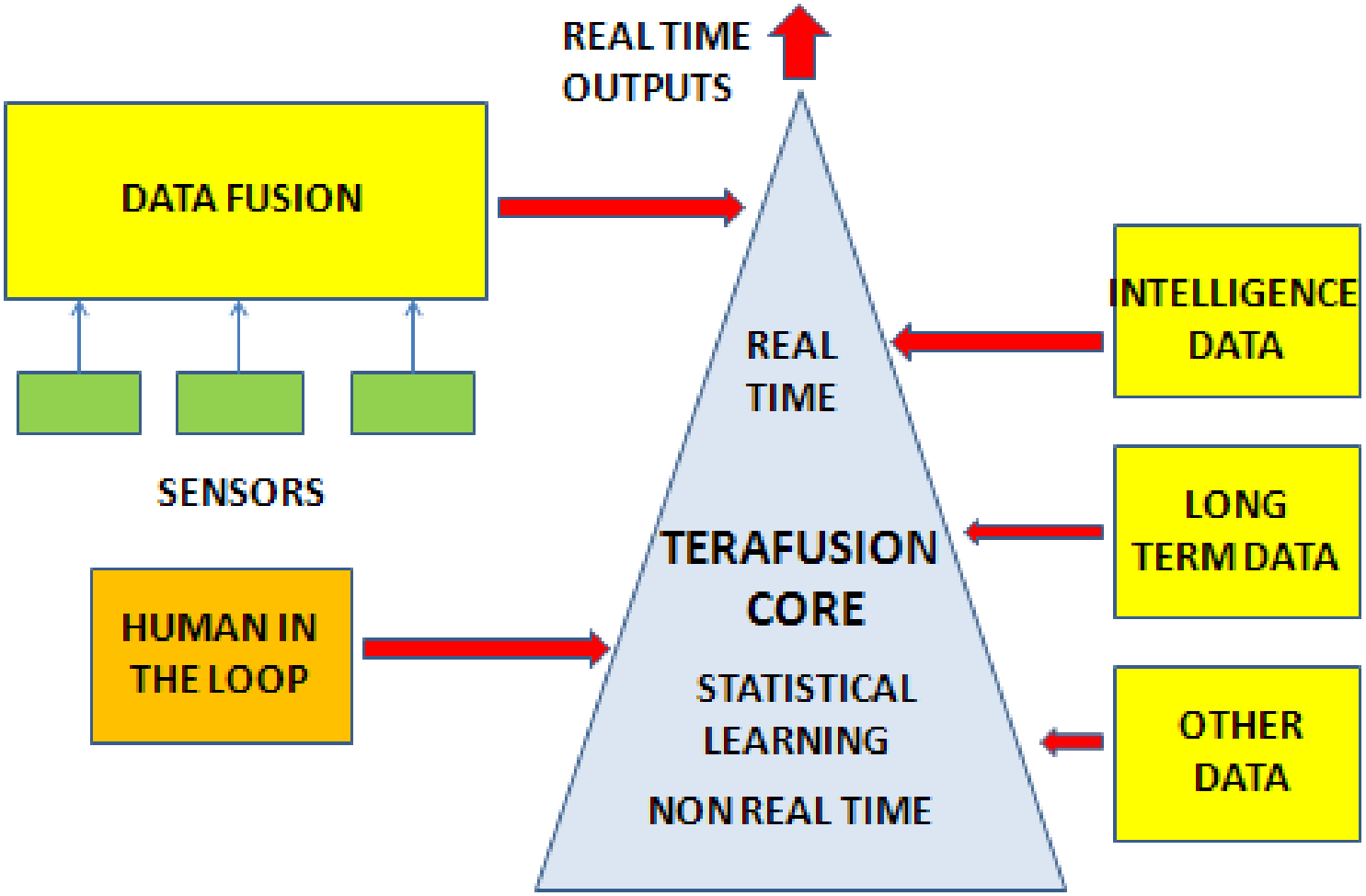
Data Fusion

Data Fusion is the process of integrating and merging multiple data and knowledge, representing the same real world object into a consistent and practical data object. The whole process is usually implemented by means of several subsequent steps, in order to transform raw data into more organized and more informative data structures.

Human in the Loop

Human in the Loop is a processing model requiring human interaction inside an automated or semi-automated process. This model is particularly required when the result of an automated process leads to a critical decision, which cannot rely only on a judgment coming from a machine.

How to Put All Technologies at Work



Why Interdisciplinary Communication for Cyber Security

Social media, usually used for leisure and social interactions, are being used also as platforms to share sociopolitical views and to mobilize support for social/ political initiatives. Cyber crime also uses these media.

Social media are online technologies and practices that people use to share content, opinions, insights, experiences, perspectives and media themselves.

They are characterized by easy access, global reach and rapid flow of multimedia information. This results in an aggregation of users with common interests.

They are virtually unlimited with respect to time and space, so they can aggregate common interests from a broad demographic spectrum.

How can we use Interdisciplinary Communication

The same tools used by hackers can be used to combat hackers.

From examination of real cases, it comes out that cyber crime is the output of a cooperative effort, carried out through extensive communication activities by using social networks.

Support to cyber crime is often offered by third parties, which have specific economic and/or political interests in causing damage to the targeted victims.

Not only technologies, but also social, political, psychological, legal, etc. factors have to be merged, in order to ensure Cyber Security.

Are we prapared for this new approach?

YES	NO
People and organizations tend to be more interactive.	This new approach requires involvement of very smart professionals.
This kind of subject has already been proposed and discussed, at least in some specialized context.	Professionals tend to work in separate areas and not to cooperate.
“Native digital” generations are more willing to accept new ideas.	Users tend to follow traditional paths and to be skeptic about new ideas.

Which are the benefits of the New Approach

To prevent illegal activities before they become effective

To manage the complex system effectively, by using a multifaceted multidisciplinary approach

To apply statistical prediction with high level of confidence

To put in effect suitable defense actions on time/ focused on the predicted threats

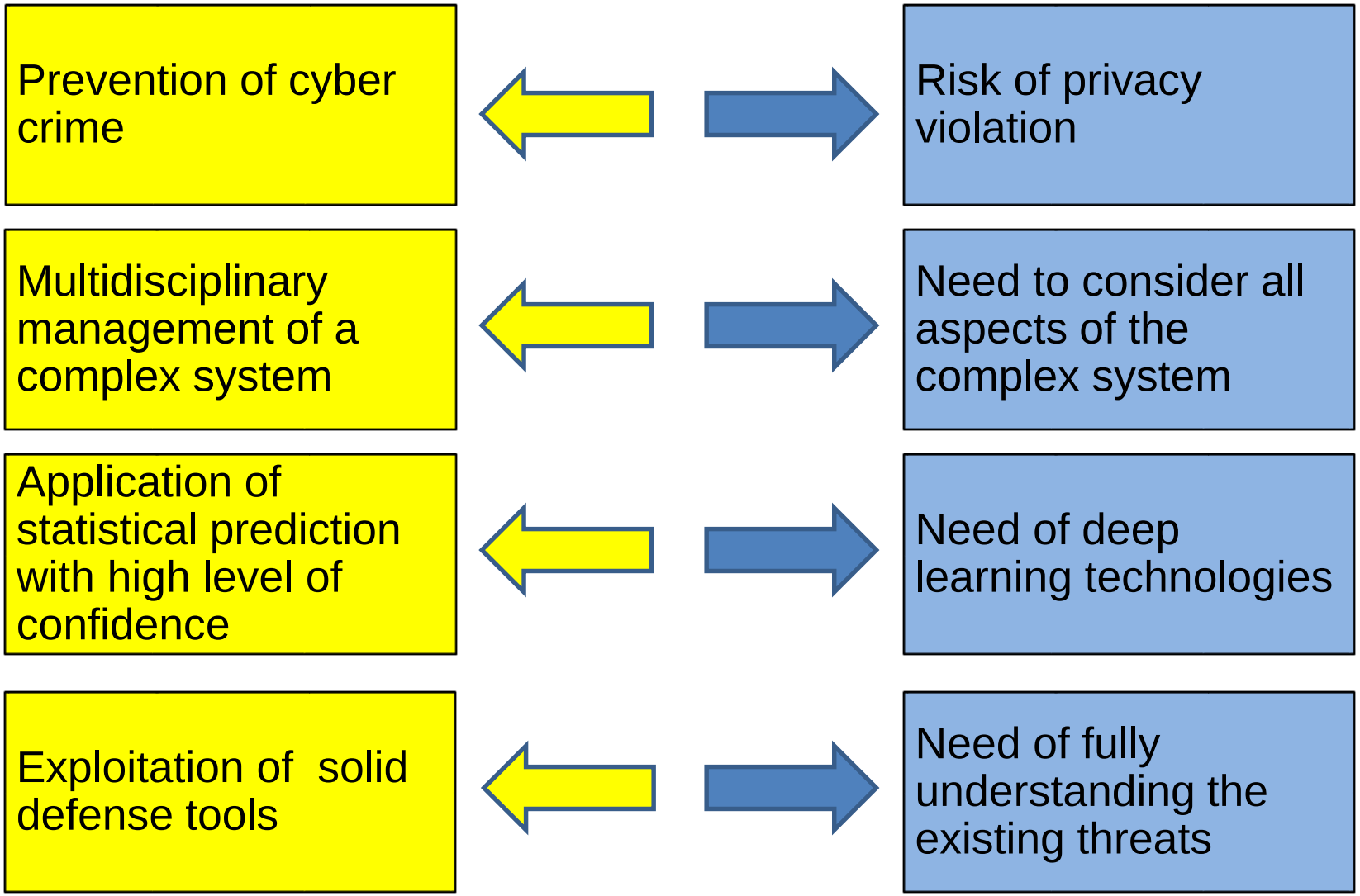
Which are the possible drawbacks

Confidence in prediction is not 100%, due to the statistical nature of the approach. But level of confidence can improve after suitable deep learning time.

Practical application of the approach may limit the personal privacy of citizen, if not safely applied.

The organizations in charge of the tools must behave correctly, in order not to violate privacy and liberty rights.

How to balance pros and cons



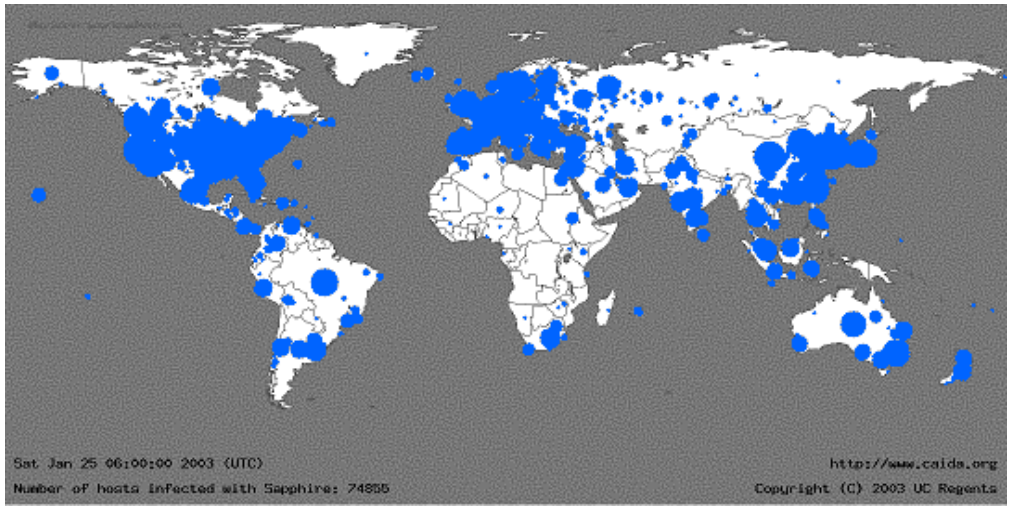
Case Study 1

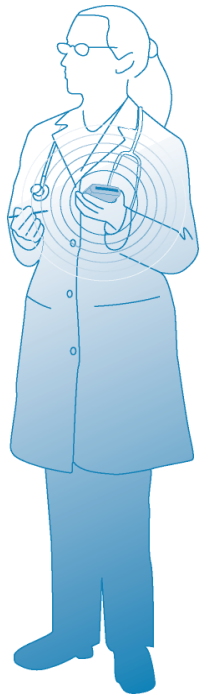
Anthem, formerly known as WellPoint, is the second largest health insurer in the US.

The company was the victim of a security breach in its customer in 2015.

The data stolen consisted of the customer data, including names, addresses, dates of birth, Social Security numbers and employment histories.

As many as 80 million customers were thought to be affected.





Causes of the breach

The hacker must have gotten the information through email phishing attempts. to get the credentials of five employees and enter the system.

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, instant messaging or other communication channels.

Typically a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as password account IDs or credit card details.

Phishing is popular with cybercriminals, as it is far easier to trick someone into clicking a malicious link in a seemingly legitimate email than trying to break through a computer's defenses. Although some phishing emails are poorly written and clearly fake, sophisticated cybercriminals employ the techniques of professional marketers to identify the most effective types of messages, the phishing "hooks" that get the highest "open" or click through rate and the Facebook posts that generate the most likes. Phishing campaigns are often built around the year's major events, holidays and anniversaries, or take advantage of breaking news stories, both true and fictitious.

Case Study 2

A “sophisticated cyber attack” on the Pentagon was conducted in July 2015, shutting down the unclassified email system for the Joint Staff for nearly two weeks and affecting roughly 4,000 federal employees (source: NBC News).

“It was clearly the work of a state actor,” Defense Department officials told NBC, without clearly stating whether elements of the Russian government orchestrated the attack, or whether it was carried out by individuals. The hackers reportedly conducted the cyber attack using encrypted accounts on social media.

No classified information was accessed or stolen, and only unclassified accounts were involved, the officials say. The Pentagon chose to shut down the system pending an investigation.

The reported attack comes roughly two months after hackers, believed to be associated with the Chinese government, successfully hacked the US Office of Personnel Management, stealing personal information about roughly 21 million people, including as many as four million federal employees with security clearances.

Conclusions and Further Steps

Critical infrastructures are strongly exposed to cyber crime.

Therefore, it is necessary to study new types of cyber security techniques, by following a multifaceted/ multidisciplinary approach.

The new approach has to be based on new technologies (big data, intelligence, deep learning, data fusion, human in the loop) and human factors.

Given the delicate aspects of human life covered by the specific topic, special care must be applied in the use of these new technologies, in order to get the maximum benefit and minimize negative side effects.