Information & Security

Alfredo M. Ronchi
vol. 44 (2020): 53-61
https://doi.org/10.11610/isij.4405

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

21st Century Cyber Warfare

Alfredo M. Ronchi

ABSTRACT:

This article provides 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 UAVs and "intelligent" rockets do not provide a significant understanding of the actual and near future scenarios. 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 ever-increasing volume of information is flowing through the network including messages concerning 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.

ARTICLE INFO:

RECEIVED: 09 Feb 2019
REVISED: 10 Jun 2019
ONLINE: 22 SEP 2019

KEYWORDS:

cyber warfare, cybersecurity, hackers, risk assessment

Introduction

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, some targeting big companies.

E-mail: alfredo.ronchi@polimi.it

Financial markets may be influenced or tilted by cyber-attacks. Smart cities and grid models must carefully take into account cyber security issues; we don't appreciate the "rebellion" of elevators or the unwanted locking of all the entrance doors of our company headquarters.

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 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. We are surrounded by "critical infrastructures" that 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, etc.

Some Recent Events

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.

The progression of cyber-attacks is amazing; let's take into account 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 [2]). Scottrade Bank data breach exposes 20,000 customer records, 60 GB MSSQL database contained customer records and other sensitive data (source CSO from IDG [3]).

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 cyberattack 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.

What Do We Term "War"?

A state of armed conflict between different countries or different groups within a country.

– Oxford living dictionaries

A conflict carried on by force of arms, as between nations or between parties within a nation; warfare, as by land, sea, or air.

– Dictionary.com

Armed fighting between two or more countries or groups.

– Cambridge Dictionary

A state of usually open and declared armed hostile conflict between states or nations: a period of such armed conflict.

– Merriam Webster

A war is a period of fighting or conflict between countries or states.

– Collins

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. 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. 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.

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 Range

Cyber Range offering a virtual environment to simulate the risk chain due to cyber -attacks and test countermeasures are a paramount, in addition they may offer force to force training sessions and identify zero days and attack vectors.

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 a European 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 platform, in line with typical simulator's features, is fed by real case study and creates 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.

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 government and private organisations.

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

cyber technologies to test existing and future mission-critical systems against cyber-attacks.

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

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

Information and Data Stream Management

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.

Proper knowledge and use of technology can support and enhance the fight against cybercrime and terrorism. 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.

European countries, relying on the expertise of academic, industry and law enforcement, may implement a holistic, interdisciplinary socio-economic approach to analyse the state of the art and trends within the cybercrime and terrorism ecosystem. The outputs of this approach will inform and guide the development and implementation of improved technological solutions. The social scientific outputs include sociological, psychological, legal, economic, linguistic and applied ethical analyses, explanations and trend characterisations of cybercrime, cybercriminals, terrorism and terrorists. In addition, security and policing insights from law enforcement will ground the approach in practical know-how to offer more complete analysis of the state of the art and projected trends.

Informed and guided by this holistic, interdisciplinary social scientific approach, data stream analysis will produce a unified security platform that enhances the ability of LEAs to monitor heterogenous, high volume data sources to identify, extract, synthesise and assess abnormal and anomalous signals (e.g. behaviours and patterns) that prefigure cyber-criminal and terroristic activities.

Risk Assessment Approach

An innovative approach in this sector is the risk assessment approach that has as core of the platform the risk assessment system (RAS). The RAS extracts, combines, analyses and elaborates signals from different data sources in near real-time. The RAS is an anomaly detection system that uses different technical tools and methodologies to analyse and process enormous volumes of data, together with improved imaging techniques to allow for the identification of suspicious events or criminals.

In a similar scenario data sources will include: 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. RAS is based on risk assessment, enhanced data analytics, machine learning and artificial intelligence.

The dashboard will offer an enhanced data visualisation and increased awareness of potential risks and cybercrime trends. The dashboard consists of an integrated user interface (UI) that will provide a clean, clear visualisation of specific potential risks together with their context. It will offer an intelligible overview of large amounts of structured and unstructured data in the context of criminal investigations. In addition to traditional visualisation formats, both textual and graphic, situational awareness in the field of complex scenario will be guarantee adopting an immersive virtual environment for sensory (visual-acoustic) data analysis by using the effect of “cognitive enhancement.”

The visualizations techniques are intended to help LEAs to 'discover' new peculiarities and properties of data that will enable them to highlights new correlations and relationships among different datasets by highlighting recurrent patterns, to monitor changes and evolutions in dynamic contexts, to provide different levels of elaboration and in-depth analysis (by zooming the view, providing additional datasets on demand, visualising different layers of information etc.).

A similar toolkit will support the LEAs crime prevention and investigation in all its various aspects, from problem setting, in which the user has to find a good way to represent/formulate the problem under study and gather new data and information, to make comparison and refinements etc., to problem solving, in which the user has a well-defined and focused goal and needs to retrieve a set of precise—even complex—information in the more effective and quick way. The Human Machine Interface (HMI) design, the techniques of data visualization and the interaction with the tool can change accordingly with the most up-to date solutions developed in different domain and for different scopes.

Information will be displayed on different interacting screen and SW/HW components (desktop, mobile, PDA, projection screens, etc) creating an immersive environment that will support the better managing of information of different nature and source, the different phases of investigation and tasks to be performed, the different relevance for the current activities and workload of the LEAs officers working under strict time constraints and in stressful condi-

tions. The RAS will provide a dynamic view on the potential threats clustered by typology, potential actors, location, level of risk, … As a complement to this, an intelligent adaptive mitigation module will suggest the proper set of counter measures to be deployed. The platform will store key information in a long-term knowledge base, providing a dynamic view on (cyber) crimes and terrorism origins and evolution together with their context.

A potential additional feature is to act as an "antenna" that will be able to identify, analyse and understand weak signals and trends related to the perception of the EU that can potentially represent threats and security issues to European countries.

Conclusions

To conclude, let us recap the key points outlined within this document, cyber technology is nowadays pervasive and at different level present all-over the globe, digital data creation in the different formats (text, graphic, audio, video, etc) are growing exponentially. As a consequence of the tight relation between cyber technology and hour everyday life 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 paramount to maximise the potential of cyber defence, one opportunity is offered by Cyber Ranges both to assess cyber infrastructures resilience, test new countermeasures, launch force to force exercises and cyber flags 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 treat in which one single man can create relevant damages globally.

References

[1] This is not even mentioning Wanna Cry and the registered domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, 2020, https://www.whois.com/whois/iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com.

[2] Hackmageddon: Information Security Timelines and Statistics, 2017, http://www.hackmageddon.com/.

[3] Steve Ragan, "Scottrade Bank data breach exposes 20,000 customer records," February 2018, https://www.csoonline.com/article/3187480/security/scottrade-bank-data-breach-exposes-20000-customer-records.html.

About the Author

Alfredo M. **Ronchi** is an expert/advisor in e-Services, General Secretary of the EC-MEDICI Framework of Cooperation and active member of the WSIS since 2003. Head of the JRC Safety, Security, Defence, and Disaster recovery and management. Mr Ronchi is member of the following Boards of Directors: Global Forum, World Summit Award, European Youth Award, European Education New Society Association, Fondazione Italiana Nuove Comunicazioni. Member of the Keio University NoE. Ronchi is appointed as an expert: European Commission, Council of Europe, Italian Association of Banks, National Research Council. He cooperated as organiser or programme chair in W3C, ACM, IEEE conferences. Author/contributor of more than 350 papers and various books on: e-Culture, IPR, e-Government, e-Health, e-Learning, e-Services. Mr. Ronchi is a professor at Politecnico di Milano.