Committee: Environment Sub-Commission 1

Issue: The environmental consequences of industrial cyber attacks

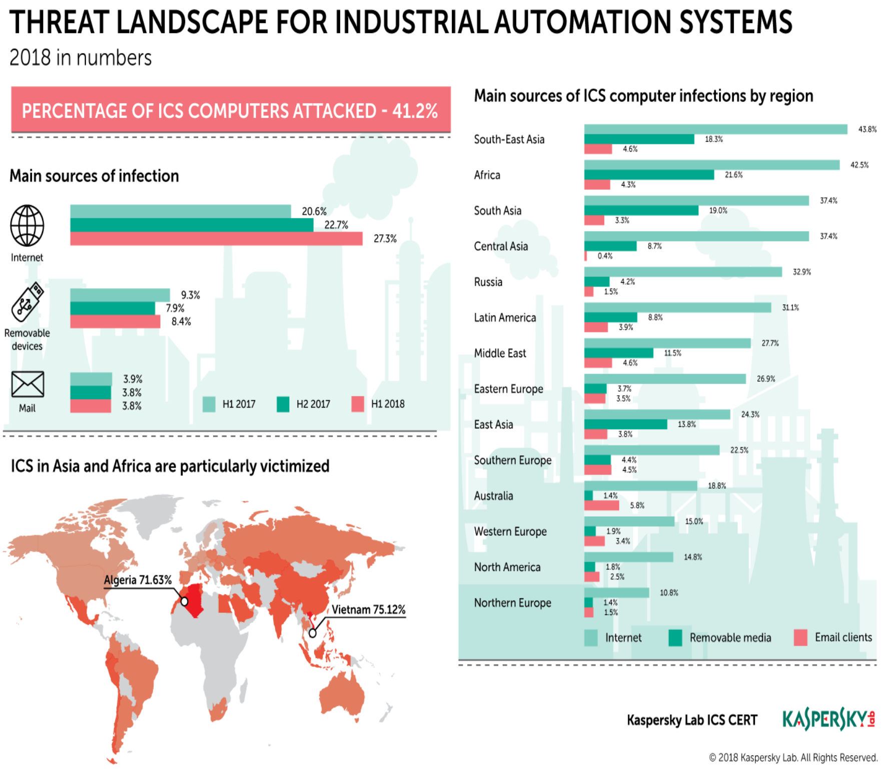
Student Officer: John Kordas

Position: Deputy President

INTRODUCTION

Since the outbreak of the first Industrial Revolution in the period 1760 to 1830, manufacturers have sought to develop new techniques and technologies in an effort to maximize their profit. The common denominator of these continuous efforts for advancement were powerful energy sources that would increase the efficiency and productivity of the machines. The first Industrial Revolution emphasized on mechanization by the use of coal along with the development of the steam engine. Moving on to the second phase of this industrial breakthrough, electric energy is witnessed for the first time and plays a cardinal in creating mass production. The third Industrial Revolution was stigmatized by the rise of a new type of energy, the nuclear energy, which surpassed its predecessors in terms of effectiveness. This particular period gave also prominence to electronics and information technology, which clearly contributed to the gradual automation of production. On the basis of the automation efforts during the third industrial revolution, we live nowadays in the era of the fourth Industrial Revolution, also referred to as Industry 4.0. This particular phase is directly correlated with the emergence of Internet, hence resulting in a new technological phenomenon, namely digitalization. The differentiator between the latest industrial outbreak and its antecedents is the fact that energy resources are of less importance and technologies such as Cloud, Big Data Analytics and Industrial Internet of Things, which contribute to automating by far the manufacturing processes.

Indubitably, the implications of digitalization in the industrial sector are enormous, since day after the means of production are being optimized and the potentials of an interconnected global system are gradually growing. Despite the increased advantages that this new virtual world offers, industrial control systems (ICS) are set in jeopardy. During the last years, the phenomenon of cyber-attacks on industrial complexes have dramatically arisen causing serious troubles in big cities and even setting the citizen's health in risk. The most common victims of such attacks are industries, which occupy themselves with hazardous materials such as refineries, power plants and water treatment facilities or pipelines. This tendency lies in the fact that these factories use highly automates technological tools, in an effort to optimize their production, and increase thus the possibility of being breached. The issue of industrial cyber-attack does not only affect the proper functioning of the factories, but it is directly connected with the wellbeing of entire cities. As a result, it is of paramount importance to address this topic effectively and eradicate the environmental consequences of such breaches.



DEFINITION OF KEY TERMS

Cyber Attack

"A cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyberattacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft."

Industrial Internet of Things (IIoT)

The term "Industrial Internet of Things" refers to the industrial electronic devices that contain censors and are connected to wireless networks so as to gather and share data, which can then be analyzed and evaluated to maximize the efficiency of business processes.

Industrial Control Systems (ICS)

Industrial Control Systems (ICS) is a general term used to describe the different types of control systems, including devices, systems and networks, which contribute to the automated operation of industrial processes.

SCADA (supervisory control and data acquisition)

SCADA is a system, which operates with coded signals through communication channels in order to provide full control of remote industrial equipment. The SCADA system is one of the most commonly used types of ICS mainly in industrial complexes that seek automated production.

Cybersecurity

Cybersecurity, also known as information technology (IT) security or electronic information security is defined as the state or practice of the defense of an individual's or entity's computers, mobile phones, networks, server, electronic systems and private information from cyber breach, which may involve threat or unauthorized use of data.

BACKGROUND INFORMATION

Historical background of SCADA system attack

Attacks on SCADA systems are a relatively new phenomenon and according to analysts the result of the fourth generation industry technology, which keeps a wide back door open for dark-side entities and sets these systems in jeopardy. A brief review of the evolution of SCADA architecture makes it possible for one to comprehend the current and past attack landscape. Malware did not pose a particular threat to the first generation, also known as "monolithic" systems due to the fact that they were not interconnected with other devices. As a result a potential intruder would have needed authorized physical access so as to interfere with them. Moving on to the second-generation SCADA systems, this type of technological architecture allows data flow across multiple stations connected via a LAN. However, during this period security against attacks was not an issue of considerable importance, since the new non-standard network protocols constituted, by far, a more critical matter. The neglected cyber security parameter enabled the appearance of SCADA malware. A characteristic example of such intrusion is an unknown Trojan program remotely inserted into a SCADA in 1982, resulting into a massive natural gas explosion along the Trans- Siberian pipeline. The malicious attacks increased significantly during the third phase of the evolution allowing the system to operate devices that are separated geographically and attached to more than one local area network, called PCN (process control network). In this period of time multiple industrial cyber-attacks took place with the Trojan program being installed in the pipeline system of a Russian oil company, thus disrupting the control of gas flows for several hours being representative example of cyber breach. The adoption of fourth generation (4.0) technology translated into even more automated industrial processes and consequently exposed SCADA systems to increased risks. Viruses such as Stuxnet, Black Energy and Havex have played a primary role in recent cyber-attacks by causing massive destructions in industrial complexes. The big number of breaches as well as the development of new malware clearly unfold the susceptibility of ICSs to potential intrusions.

ICS attack methods

Buffer overflows

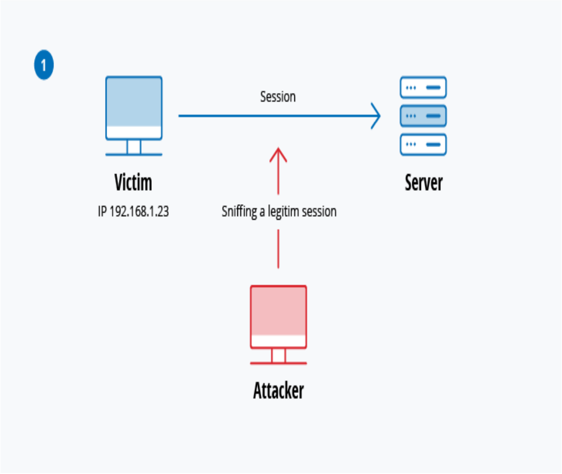
Buffer overflow occurs when a program or a process tries to store more data in temporary storage than it can actually hold. According to reports by major security companies, this particular method is responsible for approximately 25% of the attacks

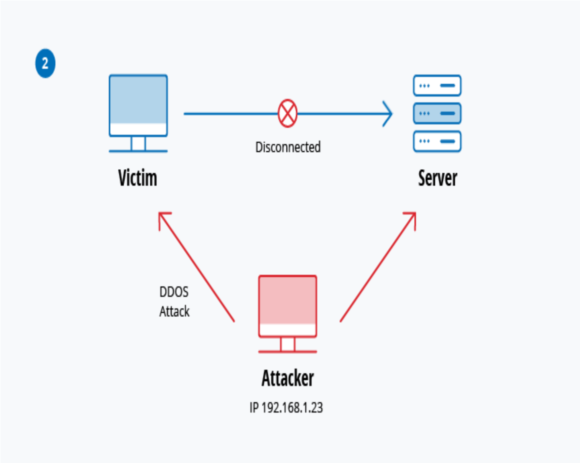
Distributed Denial of Service (DDoS)

Currently, one of the main threats to ICS are the DDoS attacks, a really broad category that can range from the loss of communication with a device to constraining or crashing certain services within the device itself (e.g. storage). Such attacks on industrial systems can have significantly negative consequences, which may involve system disconnection or even complete shutdown. A survey carried out by the Center for Strategic and International Study concludes that DDoS attacks were highly severe in the energy/power and water/sewage sectors, where attacks were usually directed to operational control systems like SCADA.

Man-in-the-middle (MitM) attack

MitM attacks pose a great threat computer software and constitute a mode of cyber breach that has evolved with technological advances. In a Man-in-the-Middle attack an intruder inserts himself in the communication channel of a client and a server, being able to read and write on the transmitted messages without either party being aware of it.





These two photos depict the procedure that a hacker must undergo so as to intercept messages exchanged between two parties.

Attacks with significant environmental implications

- In 2000, a hacker, by means of electronic messages, disabled alarms at four pumping stations managing thus to intrude into the system. This attack caused 800,000 liters of untreated sewage to flood the waterways of Maroochy Sire, Australia. The sewage spill polluted over 500 meters of open drain in a residential area and flooded into a tidal creek. The local investigator, representative of the Australian Environmental Protection Agency, reported that marine life died, the canal water turned black and the atmosphere was unbearable for the citizens.
- American security company, Verizon, reported in March 2016 a list of nearly 500 incidents that took place in 2015. Among these incidents was the hacking of computer systems of a water treatment plant and the interference with chemical processes, which set thousands of people's life in potential health dangers by drinking polluted water. According to the report the intruders gained full access to the system, hence being able to change the levels of chemicals used to treat tap water. Fortunately, the company whose identity was not revealed by Verizon, reacted quite promptly and

reversed the chemical and flow changes. Although no great damage was caused, this attack proved once again the poor cybersecurity protocol that the majority of industries possess. Verizon's report apportioned the cyber breach to the outdated operating system across the network and the fact the entire company's IT network was based on an ancient application system, dated back in 1988.

- In December 2014 the annual German Federal Office for Information Security revealed a massive attack on a steel mill in Germany causing significant damage to the complex. According to the German Agency the attackers first hacked into the office software network of the industrial site through the so called "spear phishing". In essence hackers send fraudulent emails seemingly coming from reliable sources that usually encourage the recipient to open an attached document or visit a website with malware. In the case of the steel mill it was a file, which was opened causing the injection of the malware into the software of the plant. From there, they took control over most of the industries' systems. Once they gained full access they destroyed every single mechanism that involved human operation and prevented the activation of security settings. The impact of this attack was a burn furnace, which could not be shut down in the regular way and behaving in a unconditional way resulting in massive damage to the whole system and posing a threat to the citizen's lives.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

United States of America

The United States of America deals with a huge amount of cyber-attacks every year. This explains the reason why 58% percent of the digital security organization are located and operate in this country. The government is continuously promoting transparency, productivity and development in the security field. The US has attempted coherent endeavors with accomplices in outlaying cyber security principles, addressing cyber-crime and terrorism and protecting industrial software from malware threats.

Israel

Israel is the country that takes the second largest number of cybersecurity measures and it continues its efforts on grater scale as cyberspace is getting more and more challenging. The government has allocated much of its budget on cyber issues and provides its young citizens with the necessary education as soon as middle school begins.

Algeria

Algeria is considered according to recent studies as the least prepared country for cyber-attacks in the world. This lies mostly in its huge lack of legislation and computer malware rates as well as the least possible funding of security programs.

ENISA (European Union Agency for Cybersecurity)

The European Union Agency for Cybersecurity is an agency, which was originally created and is still being operated by the EU. Its main goal is to improve network and information security in the European Union as well as the provision of assistance to Member States and the entire European business community in terms of meeting the cybersecurity requirements. ENISA has put rigorous efforts in proposing viable and effective solution for the protection of critical infrastructure and ICS SCADA systems.

TIMELINE OF EVENTS

Date	Description of Event
1982	Trojan program inserted into SCADA system program causing a massive natural gas explosion along the Trans-Siberian pipeline
2000	Maroochy Sire sewage control system in Australia attacked leading to the release of sewage
January 2003	The “Slammer” worm entered the nuclear power plant in Ohio via an infected computer connected to the plant’s network
March 2006	First SANS SCADA summit(exchange of ideas, methods and techniques for defending control systems)
2008	Establishment of Repository of Industrial Security Incidents(RISI), a database of cyber security incidents that have affected process control, industrial automation and SCADA systems
2010	The Stuxnet worm is for the first time being observed, but evidence suggests that variations of this malware date back to 2007
2011	The EU Agency for Network and Information Security (ENISA) published a report: ‘Protecting Industrial Control Systems: Recommendations for Europe and Member States’.
2012	Houston water system ICS jeopardized by undisclosed malware
2013	National Institute of standards and Technology(NIST) proposes the development of a framework to reduce cyber risks to critical infrastructure

December 2014	Massive attack on a steel mill in Germany

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

Resolution 2341(2017): The Security Council called upon Member States to address the danger of terrorist attacks, including cyber-attacks, against critical infrastructure. The resolution underlines the importance of international cooperation and expansion of knowledge on this particular issue in order for countries to better prepare themselves for a potential attack. Additionally, the Council calls upon all Member States to a legal framework concerning the accountability for attacks aimed at critical infrastructure, a term covering bridges, power lines, airports and nuclear power plants, among other facilities.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The topic of industrial cyber-attacks appeared for the first time just a few years ago and as a result no actual steps forward have been taken for the elimination of the issue. Part of MEDCs like US, Israel and Canada have fallen victims of cyber breaches a couple of times and have consequently raised a consistent cybersecurity system able to stifle potential attacks. In Less Economically Developed Countries (LEDCs) like Algeria, Tunisia and Vietnam computer security labs have prevented a big number of malicious activities against their enterprises. In terms of more deliberate measures against cyber-attacks the UN has adopted resolution 2341 which sets general goals and strategies on how the issue at hand should be approached by Member States. Similarly, the EU has put forward a number of resolution, with the one proposed in 2018 being the most updated, calling to support the European cybersecurity industry and launch a Europe-wide counterattack on ingenious intruders. The following list presents the most important EU actions to tackle cyber terrorism:

- **European Parliament resolution of 13th June 2018 on Cyber defense:** In its resolution the European Parliament welcomed the Commission's 2017 cybersecurity package and urged the EU as well as the Member States to support the European cybersecurity industry.
- **Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers:** The aim of this proposal is to help EU develop the cybersecurity

technological and industrial capacities with the objective to increase the competitiveness of the EU's cybersecurity arsenal and create an interconnected research ecosystem.

- **Protecting Industrial Control Systems, Recommendations for Europe and Member States, published on December 14th 2011 :** This report published by ENISA explicitly describes the current situation of ICS security and proposes a variety of measures, which could assist Member States in their effort to combat Industrial Cyber Attacks. The paper calls for the establishment of a pan-European strategy against ICS attacks, which sets education and raise of awareness as the primary pillars for the eradication of cybersecurity issues.
- **Industry 4.0 - Cybersecurity Challenges and Recommendations, published on May 20th 2019:** This paper is another initiative of ENISA to address the phenomenon of cyberattacks against ICSs. The report lists the different challengers the adoption of security measures and security of Industry 4.0 may present. In addition, ENISA proposes high- level recommendations on creating a durable and adapted to the needs of Industry 4.0 cybersecurity system.

Generally speaking, however, the issue needs to be addressed at its roots, since no fertile ground to build up on exists and innovative but at the same time realistic solutions should be proposed.

POSSIBLE SOLUTIONS

The issue of industrial cyber-attacks and its implications on the environment is a relatively new issue, hence no radical measures have been taken neither by Member States nor by responsible organizations. This delayed reaction to attacks on critical infrastructure can be appointed to several factors. First of all, the world of industrial is a phenomenon that appeared some years ago, during the transition of our world to the fourth technological revolution. Consequently, a great number of plants operate with outdated automation systems, whose firewall is extremely vulnerable to the newly developed malware. Moreover, the cost of upgrading the already existing or even buying new equipment is quite, hence discouraging industries from proceeding with such expenses.

Taking into account the above mentioned parameters that have partially led to the current situation in cyberspace, companies should be first and foremost get informed about the new technological challenges, since many of them undermine the importance of this issue. Members States should obviously play an active role improve related education through country-sponsored campaigns and seminars. At this point, one could argue that such a proposal could only apply to More Economically Developed Countries (MEDCs) and Less Economically Developed Countries will continue to suffer from this plague. Practical cooperation through funds and continuous exchange of information on the issue could be proven to be extremely useful for those countries that lack the necessary knowledge and infrastructure so as to protect their enterprises.

Additionally, the allocation of sufficient part of the industries' annual budget on the latest, durable systems is another parameter of significant importance in an effort to suppress the phenomenon of industrial cyber-attacks. Companies should be highly urged to collaborate with trustworthy security labs in order to install effective anti-malware systems, which will not only prevent hackers from intruding the system but also detect them so as to be punished according to the state's legal framework. Last but not least, due to the fact that elimination of cyber-attacks is indeed a really difficult and complex issue, Member States should also focus on the confrontation of the current situation. More specifically, each country should establish its own reaction mechanism with standards, however, that will be agreed upon in international meetings or set by the UN. The adoption of such a measure would stimulate a unified counterattack against hackers and tighten the bonds between Member States, key to the gradual and stable eradication of this technological plague.

BIBLIOGRAPHY

Text/blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/. Accessed 11 Feb. 2015.

Chachak, Elias. "Top 10 Countries Best Prepared Against Cyber Attacks." CyberDB, 8 July 2018, www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/. Accessed 15 Apr. 2018.

"Key Vulnerabilities of Industrial Automation and Control Systems and Actions to Prevent Cyber-Attacks | Calvo | International Journal of Online and Biomedical Engineering (iJOE)." Online-Journals.org, online-journals.org/index.php/i-joe/article/view/4888/3928. Accessed 15 Nov. 2011.

"Proposal for a European Cybersecurity Competence Network and Centre." Digital Single Market - European Commission, 19 Sept. 2018, ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre.

"Proposal for a Regulation Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers." Digital Single Market - European Commission, 19 Sept. 2018, ec.europa.eu/digital-single-market/en/news/proposal-regulation-establishing-european-cybersecurity-industrial-technology-and-research. Accessed 12 Oct. 2010.

"Security Council Calls on Member States to Address Threats Against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017)." Welcome to the United Nations, www.un.org/press/en/2017/sc12714.doc.htm. Accessed 7 Sept. 2017.

"Top 6 Countries with the Best Cyber Security Measures." Analytics Insight, 18 Feb. 2019, www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/. Accessed 15 Sept. 2013.

"Which Countries Have the Worst (and Best) Cybersecurity?" Comparitech, 12 Feb. 2019, www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/. Accessed 16 Apr. 2009.

Photos

1."404 - Page Not Found - Netwrix Blog." Netwrix Blog – IT Security Best Practices, blog.netwrix.com/wpcontent/uploads/2018/05/CA_session_hijacking. Accessed 15 Sept. 2016.

2.Kaspersky Industrial CyberSecurity, 9 ics.kaspersky.com/. Accessed Dec. 2017.