International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 3, May –June 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Impact of Malware in Modern Society

Vijayanand. C. D*, Arunlal. K. S**

*(Cyber Security Consulting System Engineer,Cisco Systems, UK.)

** (ASAP-Skill Development Executive, Quess Corp Limited, Bengaluru, India – 560103)

----------**********----------

Abstract:

In today's world most human carry at least one electronic computing device, which has a connection to the internet. Internet starting to have influence in our everyday life. Other than computers and mobile devices, traditionally standalone equipment and devices are too now connected to the internet to make them smart. Critical infrastructure of cities, healthcare and other industries (SCADA) has been connected to internet to make it smarter. Growth of internet helps to make human life easier to live. But at the same time malware and cybercrime rate is also increasing along with that. In 2016, United States council of Economic Advisers mentioned that the estimated cost of malware cost the U.S economy between $57 billion and $109 billon [1]. In this paper work, we review most common types of malware in the internet, their impact in our society, what are the motives to create a malware and the future.

Keywords **—Bring Your Own Device (BYOD), Internet of Things (IoT), Malware, Cyber-attack, Cyberspace, Cyberwarfare.**

----------**********----------

I. INTRODUCTION

Computer Software is a set of instructions for the computer to perform a sequence of arithmetic or logical operation. Electronic devices use software to interact with humans. Computer software is broadly categorised into system software and application software. System software interacts between human and computer hardware, its role as an interpreter between human and computer hardware. Application software runs on top of system software, which provides a mean to use the computer for different purpose. Software which are programmed to cause damage to a computer, user or whole system are called malicious software, also called *Malware*.

It is estimated that in 1990 around 200 to 500 viruses were discovered or known to the industry, then the number of viruses grew rapidly in few years to 50,000 in the year 2000 [2]. In 2008, based on BBC report the number of viruses grew to one million [3]. It has now grown approximately over 1.7 billion [4]. It is difficult to put an exact count on the number of actual viruses. Malware creators can use different techniques (polymorphic and metamorphic) in their code to appear a malware as a new version. It is also true that the growth of Internet is exponential since it 1990 after Tim Berners-Lee's invention of World Wide Web (WWW). It is estimated that around 3 billion users were using internet in 2016 [5] and the number is growning. Now-a-day users are not only connecting computers or mobiles devices, but any devices such as electric blubs, cars, microwave ovens, kettles, refrigerators, home security systems, fitness wearables etc to create an Internet of "*Internet of Things"* (IoT). As per IBM, IoT in nutshell "*is the concept of connecting any devices (so long as it has an on/off switch) to the Internet"* [6]. IoT has many

use cases in modern society for public safety, precious agriculture, smart homes, water distribution systems, smart meters, power grids etc. The prediction of connected devices will reach 50 billion by 2020 [7]. The rapid growth of the connected devices can raise serious thoughts on the security side of the IoT and Internet.

II. TYPES OF MALWARES

Malware is an umbrella term used to represent many forms of malicious software. Any software purposefully design for bad intention can categorised as a *malware*. Malwares aim is to harm intentionally to the computing device and the user, directly or in-directly. In a very high-level the malwares are categorised based on their behaviour. Commercial Anti-Virus (AV) and security vendors have come up with lot of names for the malware such as virus, worms, trojan horses, keyloggers, dropper, scarewares, spammers, backdoors, rootkits, spywares, adwares, ransomwares, scripts, macros etc. With respect to AV engines, each engine uses different naming format for the same virus. Though, not all AV engine use the same method to detect the virus infected files. Some AV engines scan for strings in a file, whilst some use a combination of string scanning and heuristics analysis. Irrespective of scanning method, each AV engine vendor may refer a virus in different naming format. From an experimental test, it was clear that each vendor AV engine use different naming format for the same virus, there is no naming consistency in the industry [8]. This inconsistency can create confusion for users. To avoid confusion, this paper has used the CARO (Computer Anti-virus Researchers Organisation) malware naming scheme and malware types. CARO naming scheme was created in 1991 by a committee. The main purpose of the organisation is to solve the confusion with virus names. Major companies like Microsoft [9], Trend Micro [10], Symantec etc follow CARO naming format. Having said that, most malwares have classified into more than one category. Sophisticated malwares are a package of different programs intent to perform together to achieve the objective of the hakcer. Example: Trojan horse malware cannot self-replicate, it has to combinate with worm malware to achieve the spreading objective.

Virus name is famous in IT industry and it is most used name for almost all types of malicious code. The name virus was first discussed at a security seminar by Len Adleman in 3rd November 1983 [11]. Virus usually attach itself to a program or a file. It has the capability to execute itself to inert its own code by modify other programs in a computing device. A virus program can copy itself and infect a computer device without the permission or knowledge of the user. Though it can self-execute, but it needs human action to spread. If an infected file or a program is installed or shared with a new computer, the virus will automatically copy itself into the new computer and execute its code. It spread though infected files. Broadly, most virus programs have two logical sections.One to create copy of the virus file into one or more files on the infected computer and the second part of the code is to perform the malicious intention as per programmed by the hacker. AV vendors have come up with many methods to identify the evolving malware industry. Other than traditional way to using signatures to identify the malicious code, AV companies are using behaviour monitoring, heuristics, sandboxing, emulations and even using Artificial Intelligence (AI).

Unlike virus, *Worms* have the capability to replicate itself without human action from one computer system to another. A worm does not need a host file, it does not need to attach itself to another program either to replicate. Some worms can scan the network, collect the IP addresses and replicate to the other computer using computer network. Some use contact book and sends email with infected worm file to them. CARO doesn't consider worm as a separate malware type and all worms are considered as part of virus category [12].

Trojan horse is a famous historic tale when Greeks built a large wooden horse and hide their army men inside the horse to gain access inside the city of Troy. Similarly, in cyberspace a malicious piece of code can impostor and claim to be some legitimate program, but in fact, it is a malware. It tricks the user by misleading the real intent of the software. Hence the name Trojan horse. Unlike Virus, Trojans doesn't have the capability of self-replicating. Once it become active on a computer system, an attacker can access and even control the computer remotely.

Rootkits technically need not be malicious, it has the capability to hide files and processes from other processes, applications, AV engines, even from own operating system. Commercial companies have used rootkit to restrict user behaviour [13]. The name implies, to have access at 'root' level of a system with administration tools to perform the admin tasks and the 'kit' word applies to the admin tools, hence the name rootkit. It usually installs for administration purpose on a system. The hackers utilise the rootkits to gain remote access without the information of the legitimate user of the system and to avoid the detection. Once installed, the rootkit malware can help to steal the data and resources from infected system and hide undetected for years. There are two main types of rootkits, they are divided based on where they hide and run. User-mode rootkits runs at ring 3 and kernel-mode rootkits at ring 0. Rings are privilege mechanism for the processes in x86 architecture [14].

Backdoors are closely related to rootkits. Unlike rootkits which are used for administration purposes on a system, backdoors are mainly a weakness in a system. In general, backdoor provides a way for an unauthorized user to gain access on a computer system in a stealth way. If the rootkits are not well protected (if they are installed for legitimate administrative purpose) then it could lead to open backdoor on the system. Thus, installing a rootkit may allow unauthorized access into the system. Backdoor as a malware, are very similar programs like rootkit in which an attacker can trick a user to install on his system. The main purpose of the malware is to open a backdoor connection for the hacker to access into a computer system remotely. Depends on where the backdoor malicious program installs, an attacked can gain user-level to root-level privilege access on the system. Once the hacker establishes a connection to the system via backdoor, then the hacker can steal information, control the system, modify the files, launch different forms of attacks.

Millions of devices are connected to the internet, some of the devices still have default username and password (factory default) on the devices, which can be easily compromised [15] and used as a bot. Bots are devices which are part of a larger network called *Botnet*, which is controlled remotely from a centralized command and control (C2) centre. Some botnet systems can obfuscate users to download trojan horse by misleading as free legitimate software, or as a phishing emails attachment or using other tricks. Once the bot malware infected and activated on a device, the malware will establish a connection to the C2 centre, and the device will become part of the botnet system. C2 centre has the control of the infected device and can use it to generate Distributed Denial of Service (DDoS) attack, steal sensitive information (passwords, credit card numbers, key strokes, propriety data), use computing resource for crypto mining etc. It is estimated that the quarter of all devices connected to the Internet are part of botnet system [16]. *"Botnet is an example of using good technologies for bad intentions"* - Symantec [17].

III. MALWARE ATTACKS

From 90's Electronic mail (email) system to twenty first centuries next generation of the Internet, and with the rapid growth of IoT, billions of devices are connected to the Internet. Every day more and more devices are connecting to the Internet. With the proliferation of IoT has revolutionised the public services, healthcare, automated home, smart

personal equipment, industries, agriculture, infrastructure, trade, communication, automobile etc. Current society depends on critical infrastructures and services enabled using latest technologies. Traditional cooperate way of working from office premises is changing too. Most cooperates embracing Bring Your Own Device (BYOD) and **Cloud** based applications. On-premises datacentres are moving towards Cloud. In 2018, Cloud services provider market reached $186.4 billion with a growth rate of 21.4% year-on-year [18]. Cloud based applications provide flexibility for employees to work remotely from anywhere (home, airport, coffee shop) and access to the official data anytime. This luxury of flexibility comes with new attack surface as well. Many researches have been carried out to understand the threats associated with cloud services such as visibility and remediation of vulnerabilities, data integrity, authentication weakness, risk mitigation measurements, events and incidence management, data privacy and confidentiality in a highly virtualised and multi-tenant environment [19]. Cloud security is another topic which falls out of the scope for this paper. But it is worth noting that any form of cyber-attack can have impact on the business and economic stability. And from the past incidences, it is clear that the data security breaches on confidential and sensitive information can negatively impact the stock market [20].

Broadband (Internet connection) is a common utility like electricity or water supply in every house in a modern society. Home equipment's with internet connection provides smart features than their standalone version. Smart **Home** concept is growing rapidly. As per IDC, smart home devices are expected to grow 26.9% year-over-year and as estimated shipment of 832.7 million devices in 2019 [21]. Unlike corporate offices where dedicated security professionals and security products have been deployed to defend the network, home networks usually don't have this luxury of layered defenced approach nor support from a security expert to defend any form of malicious attack. Hackers can easily exploit this weakness to launch the attack. In 2018, a malware name VPNfilter reported by Cisco TALOS which is designed to target home routers [22]. The malware is capable of maintaining a persistent presence on an infected router even after a reboot. Other than other malicious capabilities, the malware can perform man-in-the-middle (MitM) attack, sniffing all traffic transmitting through the router. It is designed to intercept the web traffic and negotiate to the end device to downgrade the SSL/TLS encryption to plaintext HTTP traffic. Plain text traffic is easy to manipulate and read. As per Symantec, it is estimated that the malware infected half a million routers in more than 50 countries [23].

A variant of malware which encrypts the Master Boot Record (MBR), Hard disk, erase files of windows operating system. Some version of the malware may encrypt only the MBR while other encrypts the hard disk, some may encrypt both Hardware and MBR. Irrespective of the encryption style, the key to decrypt needs to buy paying in bitcoins (Crypto currency) to the hacker. Hence the name *Ransomware*. There are few flavours of ransomware attack in 2017. The main ransomware malwares are WannaCry, Petya and NotPetya (NotPetya is also known as PetrWarp, GoldenEye, Petya.A, Petya.C, PetyaCry, Nyetya). WannaCry's attack vector was using a hacking tool named EternalBlue which exploits SMB protocol. **Healthcare** industry become one of the main victims of the WannaCry malware. The attack impacted around 60 National Health Service (NHS) hospitals, 595 general practices (GPs) systems and thousands of patients. Attack on the NHS computer systems led to a minimum of 7000 outpatient appointments had to cancel. The impact had reached even to the critical healthcare service department too, urgent cancer referral was delayed for 139 patients [24]. WannaCry, which had a kill switch of verifying whether a gibberish URL is active or not. Once the URL is active the ransomware becomes inactive and shutdown. This helps to mitigate the spreading of WannaCry.

Initially, malware Petya used email attachments (Phishing attack) as the attack vector, later a variant of malware Petya use EternalBlue and EternalRomance hacking tools as the attack vector and is known as NotPetya. NotPetya use Mimikatz tool as a dropper to steal the administrator password from the memory on a compromised system. It was built to spread more quickly and doesn't have a similar kill switch inbuilt into the malware code like WannaCry. May be the malware creators might have learned their lessons from WannaCry. One of the main victims of NotPetya was **Shipping industry**. Maersk shipping company had impacted the NotPetya malware forced to lock down their entire global IT system for few days. The shipping company have presence all over the world. Maersk is responsible for 76 shipping ports spread across the globe including container ships with tens of millions of tons of cargo shipmentswhich is equal to a fifth of the entire world's shipping capacity, locked down in the sea for days due to malware attack [25].

In Oct 2018, The Cybersecurity and Infrastructure Security Agency (CISA) part of Department of Homeland security (DHS) in United State of America, released a report on cybersecurity threats to precision agriculture [26]. DHS report warned about the impact on Confidentiality, Integrity and Availability (CIA) of data. **Agriculture industry** have adopted latest and advanced technologies such as remote sensors, equipment automation, global positions systems (GPS), location tracking systems, robotics, machine learning, edge computing and other communication network systems to decrease the operations cost and to increase the productivity of the farming. Agriculture not only a private business of an individual farmer, it is vitally important to the nation's overall economic and food security. The farmer community supplies food for the entire nation and also provides economic exports globally. Cyber-attack on the agriculture sector can have impact on the economy of a nation.

SCADA systems are used to control and monitor **critical infrastructure** of a state or nation, such as electricity distribution, transportation of gas, oil pipelines, water management and distribution, traffic lights and other systems in a modern society. There are known incidents recorded in RISI database which covers from trojan attack on Siberian Gas Pipeline explosion in 1982 to German steel mill cyber-attack in 2015. Advanced social engineering used as the attack vector to gain access in the German steel mill network which led to the malfunction of the furnace. Stuxnet is a famous worm had stuck the Iranian nuclear facility at Natanz in 2010, which consider as one of the most complex malwares. The Stuxnet malware was designed specifically to exploit the Siemens systems and frequency-converter drives used to power the centrifuges made by Fararo Paya in Iran and Vacon in Finland. Malware Duqu and Flame are very similar to Stuxnet malware which are also developed as a *Cyberweapon* for the disruption of critical infrastructure [27]. In 2016, Mirai malware, a cyberweapon,used IoT devices to create a large botnet system name Mirai was successful in bring down OVH cloud service provider by launching 1.1 Tbps DDoS attack [28]. The attack is considered as one of the largest DDoS attacks till today.

IV. MOTIVATION

Today's modern society is a massive sociotechnical system. Researchers have highlighted that cyber-attacks are indeed associated with social, political, economic and cultural (SPEC) conflicts [29]. Most countries are investing in technologically advanced infrastructure [30]. The critical infrastructures are the backbone of a state or a nation. It is crucial to protect during times of political conflicts and social instability. Motivation for political led cyberattacks are mostly to spread propaganda, protest against political actions, protest again certain laws, outrage against acts related to government or related organization's physical violence to the general public. In 2016, Russia's involvement in U. S presidential election was a

politically motivated attack. US Democratic National committee (DNC) candidate's private email server had been compromised. The emails were stolen and published in Wikileaks website. DNC blames Russia is responsible for the cyber-attack to influence the presidential election. Russia is blamed for 2007's DDoS attack on Estonian government and commercial websites which lasted for days. The attack impacted Estonian banks, new agencies, ministries, newspapers and broadcasters and government website [31]. The motivation for the attack was related to *cultural and political conflict* of interest. The attack originated from the disagreement between Estonian government and Russia about the relocation of the Bronze Soldier of Tallinn grave. *Socio-cultural* conflicts can also motivate cyberwar, Twain and China in 1999, Russia and Georgia in 2008, Ongoing Israel and Palestine are examples of socio-cultural triggered cyber-attacks [32].

Other than for fun and curiosity, one other main motivation for a cyber-attack is personal or corporate financial greed. *Economically motivated* attacks are usually done by cyber mercenaries, cyber criminals, organized cartels. In 2009, personal economic situations have led individuals to choose cybercrime industry. Due to economic meltdown in IT sector in China, many lost their job and turned to cybercrime activity for economical reason [33]. Recently Amazon.com Inc become victim of cyber-attack, around hundred seller accounts have been compromised and stolen the money from these accounts [34].

V. CONCLUSION

Cyber-attacks can cause significant loss of business intelligence and intellectual property, damage brand reputation, loss of money. As the number and evolving technical complexity of the malware is increasing day by day, current malware detecting mechanisms is not providing enough capabilities to keep the hackers out of the system. Moreover, the upsurge of cyber CaaS (Crime as a Service) business in dark web, even less skilled cyber-criminals can buy malware bundles to launch sophisticated attacks and the shift of cyberspace into cyberwarfare. It is clear that the cyberspace is an arm race, with one side contributing to the betterment of human life and the other side is a growing threat for the world.

VI. FUTURE SCOPE

As the Internet and the smart devices are more deeply penetrate our lives, we at personal level starting to face new privacy and security vulnerabilities. With the revolution of IoT, everything ties together from cars, our homes, phones, traffic navigation, entertainment, to our medical devices through the Internet. Cyber security become one of the critical elements in today world. As per the evolving risks landscape 2009-2019 report of the world economic forum, cyber-attack is ranked among third in 2018 and fifth in 2019 report.

There is a saying *"a chain is only as strong as its weakest link"* and it apply to the cyber security as well. Malware is constantly evolving to adapt to the changing modern technology. The new variants are more and more sophisticated, designed to exploit zero-day vulnerabilities, penetrate most security devices and avoid detection. Malwares already using techniques like polymorphic and metamorphic to change their code as they propagate to avoid detection. Advanced Persistence Threat (APT) is another method of cyber-attack, use sophisticated hacking techniques to gain access to a system and remain undetected inside the system for a prolonged period of time.

Cyber threats are getting more advanced with upsurge of highly skilled hackers and the nation-state sponsorship, led to the development of sophisticated hacking tools. In 2018, 12thMay the WannaCry ransomware attack on UK's NHS costs billions of pounds to repair the damage and the 26thMay, the NotPetya malware caused damage of billions of dollars to fix. Researchers believe that

the WannaCry is from North Korea and NotPetya is from Russia. But the underline hacking tool which used for both the cyber-attacks was developed by CIA as a cyberweapon. Nation-states are considering *cyber-as-a-weapon*, and some nations are already preparing for cyberwarfare. Similar to regular military exercises, Cybersecurity and Infrastructure Security Agency (CISA) conducts national-level cyber exercise called Cyber Storm [35], that simulates coordinated cyber-attack at large-scale impacting the U.S critical infrastructure. The exercise includes employees from private industry, federal government agencies and international partners. As the modern society becomes more and more digitally interconnected, maintaining cybersecurity will become more difficult. As per the world economic forum, "*Cyberspace has become a fifth dimension of warfare"* other than land, sea, air and space. Hence it is critical for countries to prepare and defend from related cyberwar. **Cyberwar** is not new, it has been going on over a decade, using different methods such as data leaking, DDoS, website attack. But the impact of the cyber-attacks from damaging a file on a personal computer to destabilising a corporate business overnight has now shifted to having an impact on global political and economic system. National level cyberwarfare can have more severer consequences than hacking corporate emails or leaking data. Cyberwarfare can result in pipeline gas explosion, nuclear reactor malfunction, power grid shutdown and weapon system sabotage. It was reported that Chinese government hackers had stolen 614 Gbs of data from a U.S Navy contractor [36]. Same year China-linked spy group named APT15 was involved in an attack aimed to an organisation that provides services to U.K government. The attack was targeted to U.K government departments and military technology [37].

In this digital age, some countries are considering retaliation with military option as a response for the cyber-attack on their nation. In 2019, Israeli DefenseForce claimed that they responded Hamas cyber-attack with military operation. The main concern with cyberwar is that it is still enormously complex, need new international laws and framework. With the growing concerns over the cyberwarfare, Microsoft came out with a petition to demand "*Digital Peace Now*" [38] to highlight the devastating consequences of Cyberwar that could impact the future of human, and this issue must not be ignored.

REFERENCES

[1] T. C. o. E. Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," Feb 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[2] DaBoss, "Number of Viruses," 28 Feb 2013. [Online]. Available: https://www.cknow.com/cms/vtutor/number-of-viruses.html.

[3] "Computer viruses hit one million," 10 Apr 2008. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/7340315.stm.

[4] I. M. Bushra A Al Ahmadi, "Mal Classifier: Malware family classification using network flow sequence behavior," 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8376209.

[5] M. R. Julia Murphy, "Growth of the Internet," [Online]. Available: https://ourworldindata.org/internet.

[6] J. Clark, "What is the Internet Of things?" 17 Nov 2016. [Online]. Available: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.

[7] W. E. Forum, "Is this the future of the Internet of Things?" 27 Nov 2015. [Online]. Available: https://www.weforum.org/agenda/2015/11/is-this-future-of-the-internet-of-things/.

[8] J. Mo, "What Can We Learn from Anti-malware Naming Conventions?" 05 Nov 2015. [Online]. Available: https://www.opswat.com/blog/what-can-we-learn-anti-malware-naming-conventions.

[9] "Malware names," Microsoft, 04 Aug 2019. [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/malware-naming.

[10] "New Threat Detection Naming Scheme in Trend Micro," 28 Apr 2019. [Online]. Available: https://success.trendmicro.com/solution/1119738-new-threat-detection-naming-scheme-in-trend-micro.

[11] F. Cohen, "Experiments with Computer Viruses," [Online]. Available: http://www.all.net/books/virus/part5.html.

[12] Dr. Vesselin Bontchev, "Current Status of the CARO Malware Naming Scheme," [Online]. Available: https://bontchev.nlcv.bas.bg/papers/pdfs/caroname.pdf.

[13] "Revisiting the Sony Rootkit," [Online]. Available: https://fsfe.org/activities/drm/sony-rootkit-fiasco.en.html.

[14] C. S. B. B. K. Hojoon Lee, "Lord of the x86 Rings: A Portable User Mode Privilege Separation Architecture on x86," [Online]. Available: https://arxiv.org/pdf/1805.11912.pdf.

[15] A. S. A. Mohammed Farik, "Analysis of Default Passwords In Routers Against Brute-Force Attack," 09 Sep 2015. [Online]. Available: http://www.ijstr.org/final-print/sep2015/Analysis-Of-Default-Passwords-In-Routers-Against-Brute-force-Attack.pdf.

[16] J. M. F. M. D. L. C. J. Basil AsSadhan, "Detecting Botnets using Command and Control Traffic," [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5190367.

[17] S. Employee, "What is a botnet?" [Online]. Available: https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html.

[18] B.-Y. K. Seok-Keun Yoo, "The Effective Factors of Cloud Computing Adoption Success in Organization," The Journal of Asian Finance, Economics and Business, vol. 6, 2018.
[19] A. K. M. A. Issa M Khalil, "Cloud Computing Security: A Survey," MDPI, vol. 3, 2014.
[20] L. A. G. M. P. L. L. Z. Katherine Campbell, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," 1 Jul 2003. [Online]. Available: https://content.iospress.com/articles/journal-of-computer-security/jcs192.
[21] R. L. M. S. Jitesh Ubrani, "Double-Digit Growth Expected in the Smart Home Market, Says IDC," 29 Mar 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS44971219.
[22] C. TALOS, "VPNFilter," 06 June 2018. [Online]. Available: https://blog.talosintelligence.com/2018/06/vpnfilter-update.html.
[23] Symantec, "VPNFilter malware now targeting even more router brands. How to check if you're affected.," 29 June 2018. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-vpnfilter-malware-targets-over-500000-routers.html.
[24] S. G. J. K. C. H. A. D. Guy Martin, "WannaCry—a year on," 04 Jun 2018. [Online]. Available: https://www.bmj.com/content/361/bmj.k2381.full.
[25] D. Herbener, "The Economics of Cybersecurity and Cyberwarfare: A Case Study," 05 Dec 2018. [Online]. Available: http://austrianstudentconference.com/wp-content/uploads/2019/02/ASSC-2019-Lorenzo-Carrazana.pdf.
[26] C. a. I. S. Agency, "Cybersecurity Threats to Precision Agriculture," 03 Oct 2018. [Online]. Available: https://www.us-cert.gov/ncas/current-activity/2018/10/03/Cybersecurity-Threats-Precision-Agriculture.
[27] D. C. R. Bill Miller, "A Survey of SCADA and Critical Infrastructure Incidents," [Online]. Available: https://www.researchgate.net/profile/Bill_Miller5/publication/262315594_A_survey_SCADA_of_and_critical_infrastructure_incidents/links/551ab10f0cf2fdce843695f4.pdf.
[28] C. Kolias, G. Kambourakis, A. Stavrou and J. V. Vi, "DDoS in the IoT: Mirai and Other Botnets," [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7971869.
[29] A. S,. W. M. W. S. Q. Z. P. L. Robin Gandhi, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," [Online]. Available: https://ieeexplore.ieee.org/abstract/document/5725605.
[30] C. Heathcote, "Forecasting infrastructure investment needs for 50 countries, 7 sectors through 2040," 10 Aug 2017. [Online]. Available: https://blogs.worldbank.org/ppps/forecasting-infrastructure-investment-needs-50-countries-7-sectors-through-2040.
[31] "The 2007 Estonian Cyberattacks: New Frontiers in International Conflict," 21 Dec 2012. [Online]. Available: http://blogs.harvard.edu/cyberwar43z/2012/12/21/estonia-ddos-attackrussian-nationalism/.
[32] A. S. W. M. W. S. Q. Z. P. L. Robin Gandhi, "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," [Online]. Available: https://ieeexplore.ieee.org/document/5725605.
[33] R. McMillan, "China becoming the world's malware factory," 24 Mar 2009. [Online]. Available: https://www.networkworld.com/article/2265827/china-becoming-the-world-s-malware-factory.html.
[34] J. Browning, "Amazon Hit by Extensive Fraud with Hackers Siphoning Merchant Funds," 8 May 2019. [Online]. Available: https://www.bloomberg.com/news/articles/2019-05-08/amazon-hit-by-extensive-fraud-as-hackers-siphoned-merchant-funds.
[35] "Cyber Storm VI: National Cyber Exercise," [Online]. Available: https://www.dhs.gov/cisa/cyber-storm-vi.
[36] "Chinese Government Hackers Steal Trove of U.S. Navy Data: Report," 08 Jun 2018. [Online]. Available: https://www.securityweek.com/chinese-government-hackers-steal-trove-us-navy-data-report.
[37] "China-Linked Spies Used New Malware in U.K. Government Attack," 12 March 2018. [Online]. Available: https://www.securityweek.com/china-linked-spies-used-new-malware-uk-government-attack.
[38] "Microsoft Digital Peace Now," [Online]. Available: https://digitalpeace.microsoft.com/know-the-issue/.

