Table of Contents

Letter from the Under-Secretaries-General

Most Esteemed delegates,

It is our utmost pleasure to welcome you all to the 3rd annual edition of Ipekçilik International Model United Nations. Our names are Rana Yolcu and Fatma Erva Demir and we are sophomore students studying at Bursa Ipekçilik Anatolian Imam Hatip High School. During the committee, we will be hosting and gladly serving you as the Under-Secretaries-General of Special Committee on Cyber Security and we feel that this is a great opportunity for being a part of this great MUN activity.

Special Committee on Cyber Security aims to find solutions to very recent problems that are not provided cybersecurity and overuse of personal data, faced by the globe. Delegates will be discussing these issues and trying to find solutions. We highly recommend delegates to read and understand the study guide clearly before the conference. We also recommend delegates to think and find some possible creative solutions to have high qualified debates and speeches during the committee. We are sure that unexpected crises will make the committee more enjoyable and fruitful. We believe in you all and we cannot wait to see you all in the conference.

Lastly, we would like to thank all of the people who work too hard and prepare for this conference and let us be a part of it. But specifically we would like to thank our Academic Head Zeynep Sökücü for her great attention to us.

If you have any kind of questions, do not hesitate to ask your Under-Secretaries-General via e-mail.

Best Regards,

Rana Yolcu / ranayolcu321@gmail.com

Fatma Erva Demir / ervaademir03@gmail.com

For Position Papers: Muniacybercommittee@gmail.com

Under-Secretaries-General of Special Committee on Cyber Security

INTRODUCTION TO THE COMMITTEE

As time passes, technology and its implements such as the internet and mobile devices are developing and their services and conveniences provided to the users have made technological devices a huge part of our daily lives. Daily human life started to depend on technology, just on a mobile device, there are a lot of data such as identity information, health information, credit card, and passwords, private addresses, phone numbers, personal pictures and videos, password and user name information used to access social networks, etc. belonging to the user. If just mobile device contains this much information, technology as whole includes even more and this attracts malicious people who aimed to reach and steal private information to use them illegally on needed fields such as fake identity creation. While the benefits of technology and information on cyberspace are increasing, at the same time cyber-attacks and being a hacker are becoming more common among society. This creates non-negligible vulnerable systems the functioning of institutions, potentially endangering them and even undermining the sovereignty of the State.[1]

Cyberspace contains a huge field, due to this having an ensured place needs a global help which means combined work of governments, organizations (inventors

[1] http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf

or developers of technological devices or applications), and individuals are needed and each one of them has its own role on this.

a. **Country governments'** role is to make a political will to devise and implement a strategy for the development of digital infrastructures and services which includes a coherent, effective, verifiable and manageable cybersecurity strategy.

b. **Organizations'** role is to create devices or applications which is protected by advanced security infrastructure that enables hackers to attack and don't have security bug.

c. **Individuals'** role is to have knowledge about cyber-attacks and know how to use technical devices safely.

Cyber-attacks are a great risk for countries, organizations and individuals and it is getting more common with everyday passing. And this committee will try to find possible solutions to prevent these attacks with the help of the country, application and organization delegates.

KEYWORDS

1. **A computer hacker** is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.
2. A **computer network** is a set of connected computers. Computers on a network are called **nodes**. The connection between computers can be done

via cabling, most commonly the Ethernet cable, or wirelessly through radio waves. Connected computers can share resources, like access to the Internet, printers, file servers, and others. A network is a multipurpose connection, which allows a single computer to do more.

Networks are used to:

- Facilitate communication via email, video conferencing, instant messaging, etc.
- Enable multiple users to share a single hardware device like a printer or scanner.
- Enable file sharing across the network.
- Allow for the sharing of software or operating programs on remote systems.
- Make information easier to access and maintain among network users.

3. Cyber Security Incident: An incident is any event that threatens the security, confidentiality, integrity, or availability of information assets, information systems, and/or the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Incidents may include but are not limited to:

- Unauthorized entry
- Security breach or potential security breach
- Unauthorized scan or probe
- Denial of service
- Malicious code or virus

- Networking system failure (widespread)
- Application or database failure (widespread)[2]

4. Data, is any set of characters that is gathered and translated for some purpose, usually analysis. It can be any character, including text and numbers, pictures, sound, or video. If data is not put into context, it doesn't do anything to a human or computer.

- İnformation is an upper form of data, evaluated, analyzed, edited and transformed into a logical form.

5. Cyber entity: Tools, processes, documents, plans, projects, documented thoughts, data or information contained in cyber environments.

6. Cyberspace, refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks that employ TCP/IP[3] protocol to aid in communication and data exchange activities.

7. A Firewall, is a defensive technology that is focused on to keep bad guys out from one's network. It acts as a virtual barrier that protects both internal and external cyber-attacks that might attack your personal computer.

---

[2] http://eweb.cabq.gov/CyberSecurity/Additional%20Security%20Documents/Reporting%20a%20Cyber%20Security%20incident.pdf

[3] TCP/IP, or the Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private network (an intranet or an extranet).

The entire internet protocol suite -- a set of rules and procedures -- is commonly referred to as TCP/IP, though others are included in the suite. TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination.

TCP/IP requires little central management, and it is designed to make networks reliable, with the ability to recover automatically from the failure of any device on the network.

It keeps a check on all the unauthorized access to or from a private network and also determines which entry should be allowed or not to interact with your computer. [4]

8. The Dark Web & Darknets: The Dark Web is used to describe an encrypted network built on top of the internet which can only be accessed using specialized software. The term Darknets can also be used to describe these networks. Websites found here are not indexed; therefore, the dark web is within the deep web. These networks are described as dark, due to the characteristics that assist users in hiding their identities and the popularity of supporting illegal activities. Darknets can either be in the form of privacy networks, such as Tor or Freenet, or in the as peer-to-peer networks, such as I2P or friend-to-friend networks. These forms of networks rely on routing traffic over the network through layers of encryption to support anonymity of the users.

9. Vulnerability is a term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

10. Cyber weapon is a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings.

11. IT (İnformation Technologies): Set of tools, processes, and methodologies (such as coding/programming, data communications, data conversion, storage and retrieval, systems analysis and design, systems control) and associated equipment employed to collect, process, and present information.

[4] https://tweaklibrary.com/40-cyber-security-terms-you-should-be-knowing/

12. Botnet: A botnet is a collection of internet-connected devices, which may include PCs, servers, mobile devices and internet of things devices that are infected and controlled by a common type of malware, although users are often unaware of it.

13. Industrial espionage is the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. Industrial espionage is conducted by companies for commercial purposes rather than governments for national security purposes. Industrial espionage may also be referred to as "corporate spying or espionage," or "economic espionage."

14. Cyber Spying: Cyber spying is the act of engaging in an attack or series of attacks that let an unauthorized user or users view classified material. These attacks are often subtle, amounting to nothing more than an unnoticed bit of code or process running in the background of a mainframe or personal workstation, and the target is usually a corporate or government entity. The goal is typically to acquire intellectual property or government secrets.

15. Malware: Malware is short for *mal*icious soft*ware*, meaning software that can be used to compromise computer functions, steal data, bypass access controls, or otherwise cause harm to the host computer. Malware is a broad term that refers to a variety of malicious programs.Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

16. Hardware: Hardware is best described as a device, such as a hard drive, that is physically connected to the computer or something that can be physically touched. A CD-ROM, computer display monitor, printer, and video card are all examples of computer hardware.

17. Software: Software is a general term used to describe a collection of computer programs, procedures, and documentation that perform some task on a computer system. Practical computer systems divide software systems into three major classes: system software, programming software, and application software.

18. (General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. The GDPR came into force on 25 May 2018 and sets out requirements for how organizations need to handle personal data. It forms part of the data protection regime in the UK, together with the new Data Protection Act 2018 (DPA 2018).)

AGENDA ITEM: Restricting the usage of personal data and ensuring the cyber security

A. Ensuring the cyber security

Cyber-security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its

designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

- **Information security** protects the integrity and privacy of data, both in storage and in transit.
- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons are vital for the security of any organization.

1. Importance of cybersecurity

Cybersecurity is important because the government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information, whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing business, and cybersecurity describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber-attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. Cybersecurity is not optional. It must form part of the design of every product, of every database, of every electronic communication.

2. Threats to cybersecurity

As technology continues to evolve so also the opportunities and challenges it provides. We are at a crossroads as we move from a society already entwined with the internet to the coming age of automation, Big Data, and the Internet of Things. But as a society that runs largely on technology, we are also as a result dependent on it. And just as technology brings ever greater benefits, it also brings ever greater threats: by the very nature of the opportunities it presents it becomes a focal point for cybercrime, industrial espionage, and cyberattacks. Therefore, protecting cybersecurity is of paramount priority. And the next part is about some problems and necessities that we face and need recently;

• Cybercrime comes in a variety of forms ranging from denial of service attacks on websites through to theft, blackmail, extortion, manipulation, and destruction. The tools are many and varied, and can include malware, ransomware, spyware, social engineering, and even alterations to physical devices (for example, ATM skimmers).It's no surprise then that the sheer scope of possible attacks is vast, a problem compounded by what's known as the attack surface: the size of the vulnerability presented by hardware and software.

• Attack vectors such as botnets, autonomous cars.

• Threats including data manipulation, identify theft, and cyberwarfare.

• The need for more collaboration in order to mitigate threats.

• Inadequate level of education and awareness

-Cybersecurity isn't just about technological defenses: it's also about people. From the home user through to industry and government, everyone needs a basic understanding of cyber threats and how to recognize them.

• Need for the balance between privacy and security.

• Lack of preparation and planning

- Cyber security is not something that we can wait to protect it until there is a cybercrime. All devices must be pre-ensured to avoid problems during the attack.

B. Restricting the usage of personal data

Today, thousands of companies from various industries collect, analyze, acquire, share, trade, and utilize billions of people's personal information at unprecedented levels. Their unilateral and extensive access to data about the characteristics, behaviors, and lives of billions allows them to constantly monitor, follow, judge, sort, rate, and rank people as they see fit.

Not too long ago, the scale and depth of personal information in the hands of commercial entities was quite limited and rather easy to oversee. Credit bureaus, direct marketing firms, and businesses selling products and services to consumers started to collect, manage, and exchange data on people decades ago. That is not to say that people being numbered, rated, and ranked didn't have consequences for many in the past; however, earlier consumer databases were isolated, updated slowly, and captured only a fraction of a typical person's life. Fast-forward to the year 2017 and the situation has changed dramatically. Since the rise of social networks, smartphones, and online advertising, a wide range of companies has started to monitor, track, and follow people across virtually all aspects of their lives. Today, the behaviors, movements, social relationships, interests, weaknesses, and most private moments of billions are constantly recorded, evaluated, and analyzed in real-time which enables users to have privacy on social network.

When surfing the web, hidden pieces embedded in software transmit information about the websites visited, navigation patterns, and sometimes even keystrokes, scrolls and mouse movements to hundreds of third-party companies. Similarly, when carrying a smartphone, rich information about the user's everyday

life not only flows to Google, Apple, and a variety of app providers, but also to a significant number of third-party companies, again based on hidden software embedded by app providers. Such information may include a person's contacts, information about real-time app usage and movements, as well as data from all kinds of sensors recording motion, audio, video, and more. Furthermore, as a rapidly increasing number of devices connects to the internet – from wearables, e-readers, TVs, game consoles, toys, baby monitors, printers, and voice-controlled speakers to thermostats, smoke alarms, energy meters, door locks, and vehicles – personal data collection threatens to become ubiquitous and totalizing. Already now, though, individuals can see only the tip of the data and profiling iceberg. Most of it occurs in the background and remains opaque; as a result, most consumers, as well as civil society, journalists, and policymakers, barely grasp the full extent and forms of corporate digital tracking and profiling. Furthermore, much of these happens invisibly, often with neither knowledge nor consent of the subjects. Companies inform people incompletely, inaccurately, or not at all about their data practices. They use ambiguous, misleading, and obfuscating language in both user interfaces and contracts such as privacy policies and terms of service. Moreover, companies systematically trick consumers into data contracts. Also it is not only because of the industry's non-transparency also having a huge personal data ecosystem.

The more digital technology and personal data collection become part of everyday life, the more pervasive and opaque such practices become. While companies have used consumer's zip codes to decide whether or not to market certain products or services to them in the past, today they may use digital records about many other kinds of attributes and behaviors of consumers to make

those decisions. Apart from discriminating against people by providing some with more expensive offers than others – or by excluding them outright – there are many further ways to underserve people and keep them away, ranging from pre-filtering marketing and advertising to prioritization in call centers or ticketing systems. Conversely, companies may focus on customers with a tendency to incur late payment costs or other penalties. Briefly, automated decision-making systems exist in order to treat people differently on the basis of information about them. As a result, individuals get excluded from certain opportunities, become subject to further investigation, or are filtered out in advance. Furthermore this monitor people's choices, life-chances and systematically influence people's behavior. Also according to their interests, companies treat them differently and nudge them into overconsumption, and charge each consumer the most he or she may be willing to pay

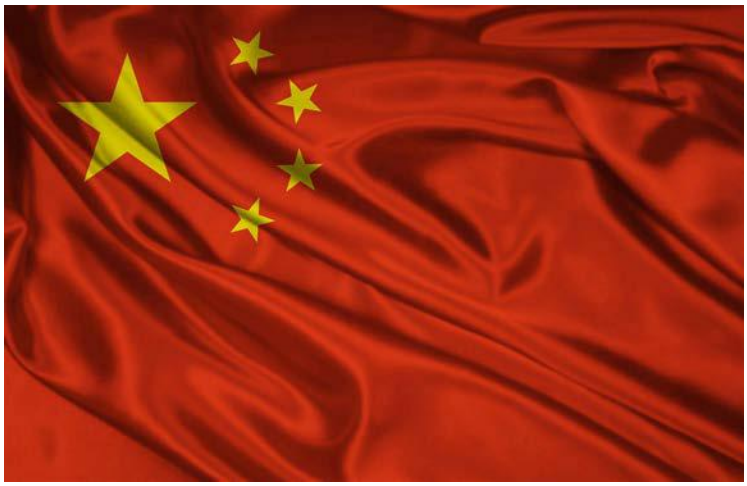
Today's large online platforms, such as Google and Facebook, have extensive information about the everyday lives of billions of people around the globe. They are the most visible, pervasive, and – aside from online advertisers and intelligence contractors – perhaps the most advanced players in the personal data business. However, in contrast to popular belief, they do not directly, for the most part, sell and share their detailed digital consumer profiles to third parties, at least not in the form of unified dossiers. Instead, the large online platforms mostly let other companies utilize their data without fully transferring it, and they let them use their infrastructure to collect more data, to the benefit of both the client companies and the platforms themselves.

Scientific studies have shown that many kinds of personal characteristics can be inferred from transactional and behavioral data such as web searches, browsing

histories, product purchases, Facebook likes, and viewing or listening behaviors. For example, personal attributes such as ethnicity, religious and political views, relationship status, sexual orientation, and alcohol, cigarette, or drug use as well as personality traits such as emotional stability, life satisfaction, impulsivity, depression, and “sensationalist interest” can be inferred reasonably accurately from collected data. Personality traits can also be inferred from information about the websites someone has visited, as well as from phone call records and mobile app usage. Information about someone’s occupation and educational level can be inferred from the browsing history. Canadian researchers have even successfully predicted emotional states such as confidence, nervousness, sadness, and tiredness by analyzing the rhythm of typing patterns on a computer keyboard.

COUNTRIES’ POSITION

1. CHINA:



China is resolutely moving forwardwith development of its own IT industry. It is also isolating itself frominternational IT technology. By exercisingcontrol over major state-run businesses, the PRC is also maintaining its sovereign position in the IT sector.

The Chinese government has issued close to 300 new national standards related to cybersecurity over the past several years.

These standards cover a range of information and communications technology (ICT) services as well as products including software, routers, switches, and firewalls.

The Cyber Security Law of the People's Republic of China, commonly referred to as the China Internet Security Law, was enacted to increase cybersecurity and national security, safeguard cyberspace sovereignty and public interest, protect the legitimate rights and interests of citizens, legal persons and other organizations and promote healthy economic and social development. China Internet Security Law was enacted by the Standing Committee of the National People's Congress on November 7, 2016 and was implemented on June 1, 2017.

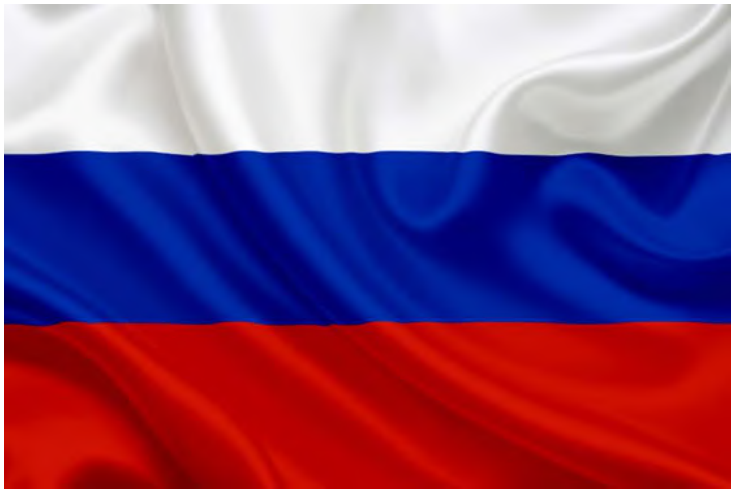
The Cyberspace Administration of China (CAC):

The Cyberspace Administration of China, also known as the Office of the Central Cyberspace Affairs Commission is the central Internet regulator, censor, oversight, and control agency for the People's Republic of China.

The CAC is in charge of cyberspace security and internet content regulation, major functions are directing, coordinating and supervising online content management and handling administrative approval of businesses related to online news reporting.

The CAC was founded in 2014. As of August 2018, the agency is headed by Zhuang Rongwen. The CAC answers to the Central Cyberspace Affairs Commission, which is headed by Communist Party General Secretary Xi Jinping.

2. RUSSIA :



On 10 September 1986, Cliff Stoll, a systems administrator at the Lawrence Berkeley National Laboratory in California, called Chuck McNatt at the computer center of the Anniston Army Depot in Alabama to inform him that ahacker called 'Hunter' was breaking into his computer systems. The hacker wanted to extract information from the US Army Redstone Rocket test site on US missile tests related to President Ronald Reagan's flagship Strategic Defense Initiative, nicknamed 'Star Wars'. This was one of the first known cyber espionage operations engineered by Moscow, in cooperation with East Germany, against the US military.

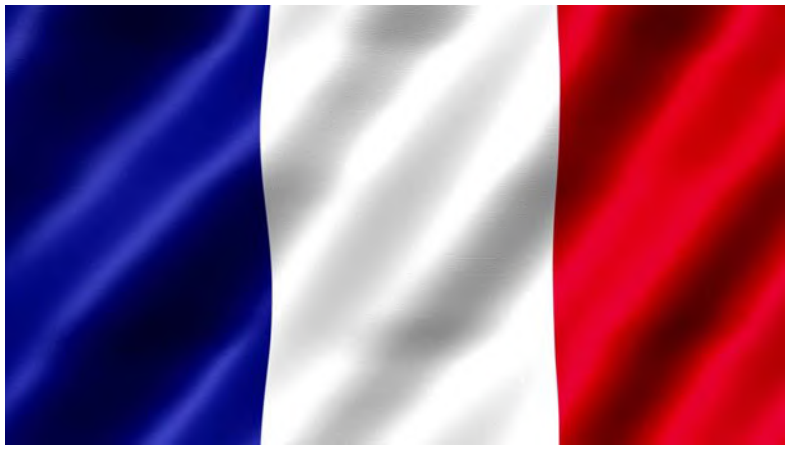
In 2017, advanced persistent threats (APTs) of Russian origin received considerable attention in Europe. The German government reportedly suffered a large-scale cyberattack, when the Russian hacking group APT28 placed malware in a government network and infiltrated both the foreign ministry and the defense ministry. Also, to cite just a few examples, Norway, Denmark, the Netherlands and Italy have accused Russia of advanced cyber espionage. For example in Norway, according to the Norwegian security service, democratic institutions, the Police Security Service and the country's Radiation Protection Authority have been

targeted. German intelligence officials have accused Russia of hacking the German government's computer networks as well as those of national energy firms. These cyber espionage and hacking activities – targeting governments, political entities and EU institutions in order to extrapolate and collect classified information – suggest that sophisticated cyber espionage and data manipulation operations are being conducted in the EU.

Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications:

The Federal Service for Supervision of Communications, Information Technology and Mass Media or Roskomnadzor is the Russian federal executive body responsible for control, censorship, and supervision in the field of media, including electronic media and mass communications, information technology and communications functions control and supervision over the compliance of personal data processing requirements of the legislation of the Russian Federation in the field of personal data, and the role of co-ordinating the activities of radio frequency service. It's an authorized federal executive body for the protection of human subjects of personal data. It is also the body administering Russian Internet censorship filters. Basically its areas include electronic media, mass communications, information technology and telecommunications; overseeing compliance with the law protecting the confidentiality of personal data being processed; and organizing the work of the radio-frequency service.

3. France:



France is fully committed to thedigital transition. Boasting a highly connected population, buoyed by sustained growth in its digital economy, France draws on talents and strengths on the cutting edge of European and global innovation.

The ‘Actions to promote the digital Republic’ planned by the French government are intended to promote their values, their economy and protect their citizens. By reinforcing digital security, France favors the development of a cyberspace that provides a sustainable source of growth and opportunities for French companies, thus asserting their democratic values and safeguarding their citizens’ digital lives and personal data.

National Commission on Informatics and Liberty (CNIL):

In the digital world, the National Commission on Data Processing and Freedoms (CNIL) is the organizer of personal data. It supports professionals in their compliance and helps individuals to check their personal data and exercise their rights. National Commission on Informatics and Liberty is an independent French administrative regulatory body whose mission is to ensure that data privacy law is applied to the collection, storage, and use of personal data. Its existence was established by the French loi n° 78-17 on Information Technology, Data Files and Civil Liberty of 6 January 1978, and it is the national data protection authority for France

In France, CNIL, a government agency that controls the privacy of personal data, has fined Google 50m euros for failing to provide clear information about the use of users' personal data under the General Data Protection Regulation (GDPR).

4. United Kingdom:

Since 2010 the Government has categorized major cyber-attacks on the UK and its interests as a top-tier threat to national security. The impact of technology, and especially of cyber threats, was identified as one of the Four "particular challenges likely to drive UK security priorities for the coming decade" in the 2015 National Security Strategy and Strategic Defense and Security Review 2015 (2015 NSS & SDSR). Its importance was reaffirmed by the Government's National Security Capability Review in March 2018.

The past year has seen cyber-attacks on the health, telecommunications, energy and government sectors in the UK. The May 2017 WannaCry attack, which affected National Health Services (NHS) for several days, should serve as a stark warning of the implications of such an attack for national security.

The Information Commissioner Office (ICO):

The Information Commissioner is an independent official appointed by the Crown. The Commissioner's decisions are subject to appeal to an independent

tribunal and the courts. The Commissioner's mission is to "uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals".

Since Elizabeth Denham was appointed UK Information Commissioner, the ICO has undertaken high-profile investigations into Equifax, Yahoo, Talk Talk, Uber, and Facebook; issuing the maximum fine under the Data Protection Act 1998 of £500,000 to Facebook, for breaches of data protection law. Denham has also overseen the conclusion of the ICO's investigation into charities' fundraising activities and a series of fines for companies behind nuisance marketing.

Elizabeth Denham has welcomed the introduction of the General Data Protection Regulation (GDPR) that came into effect on May 2018, as well as the Data Protection Act 2018.

5. UNITED STATES OF AMERICA:

As a major developed economy, the United States is highly dependenton the Internet and therefore greatly exposed to cyber-attacks. At the same time, the United States has substantial capabilities in both defense and power projection thanks to comparatively advanced technology and a large

military budget. Cyber warfare presents a growing threat to physical systems and infrastructures that are linked to the internet. Malicious hacking from domestic or foreign enemies remains a constant threat to the United States. In response to these growing threats, the United States has developed significant cyber capabilities.

The United States Department of Defense recognizes the use of computers and the Internet to conduct warfare in cyberspace as a threat to national security, but also as a platform for attack.

In April 2015, the U.S. Department of Defense (DoD) published its latest Cyber Strategy building upon the previous DoD Strategy for Operating in Cyberspace published in July 2011. The DoD Cyber strategy focuses on building capabilities to protect, secure, and defend its own DoD networks, systems and information; defend the nation against cyber-attacks; and support contingency plans. This includes being prepared to operate and continue to carry out missions in environments impacted by cyber-attacks.

Attacks on other nations:

i. China:

In 2013, Edward Snowden, revealed that the United States government had hacked into Chinese mobile phone companies to collect text messages and had spied on Tsinghua University, one of China's biggest research institutions, and the China Education and Research Network (CERNET). He said U.S. spy agencies have been watching China and Hong Kong for years.

According to classified documents provided by Edward Snowden, the National Security Agency (NSA) has also infiltrated the servers in the headquarters of Huawei, China's largest telecommunications company and the largest telecommunications equipment maker in the world. The plan is to exploit Huawei's technology so that when the company sold equipment to other countries—including both allies and nations that avoid buying American products—the NSA could roam through their computer and telephone networks to conduct surveillance and, if ordered by the president, offensive cyber operations.

ii. Russia:

In June 2019, Russia has conceded that it is "possible" its electrical grid is under cyber-attack by the United States. The New York Times reported that American hackers from the United States Cyber Command planted malware potentially capable of disrupting the Russian electrical grid.

The National Cyber Security Division (NCSD):

The National Cyber Security Division (NCSD) is a division of the Office of Cyber Security & Communications, within the United States Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Formed from the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center, and the National Communications System, NCSD opened on June 6, 2003. The NCSD mission is to collaborate with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the

civilian government and private sector critical cyber infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents.

6. Germany:

The German approach to cybersecurity strategy has developed from a civilian preventive one to a more comprehensive one, which today includes strategic military aspects. The first phase (1991 to 2011) marks the emergence of cybersecurity as a strategic issue in the context of critical information infrastructure protection. In the second phase (2011 to 2016), the government consolidated existing policies after adopting its first national cybersecurity strategy in 2011. The Snowden revelations in 2013 lifted cybersecurity sharply up the political agenda. In the third phase, from 2016 to early 2018, Germany adopted its second national cybersecurity strategy that outlines a comprehensive approach to cybersecurity, as well as a national defense strategy, which for the first time emphasized the strategic military dimension of cybersecurity within a hybrid warfare context. In 2017 and 2018, intensified discussions about the offensive aspects of government hacking indicated a further turn in toward a more expansive cybersecurity policy.

The Federal Commissioner for Data Protection and Freedom of Information:

Its task is to ensure data protection in an increasingly digital world. By this, they protect your fundamental right to privacy and your right to your own data from access by international corporate groups and also by public authorities. This is the prerequisite for a free democratic society and prevents improper advantages by corporate groups. Furthermore, they ensure that you are granted your right of inspection of records and administrative files from public authorities.

7. JAPAN

Japan has a dedicated cybersecurity law called the Basic Cybersecurity Act, which was enacted on 6 November 2014 (and promulgated on 12 November 2014). The Basic Cybersecurity Act is the first cyber security-specific law that has been enacted among the G7 nations.

The primary task of the Basic Cybersecurity Act is to ensure cybersecurity while also ensuring the free distribution of information. It is the purpose of the Basic Cybersecurity Act to move cybersecurity-related policies forward comprehensively and effectively, and contribute to the creation of a more energetic and continuously developing economic society, consequently contributing to the national security of Japan.

The Personal Information Protection Commission (PPC):

The duties of the Personal Information Protection Commission (PPC) are the protection of the rights and interests of individuals while taking into consideration

proper and effective use of personal information. It was established on January 1, 2016 to replaces the Specific Personal Information Protection Commission. The PPC is one of the highly independent organs in the Japanese legal framework. Based on the Act on the Protection of Personal Information, the Chairman and Commission members exercise their authorities independently.

8. South Korea:

The threat of cyber-attacks is increasing and as internet-enabled products become even more commonplace, the attacks become more sophisticated and serious. South Korea is the world's most wired nation, yet they are a nation without a cyber security strategy. Until now. The ransomware "WannaCry" attack in May 2017 shook the Koreans awake to the notion that their society was being attacked at every possible vulnerability, not just with physical arms, but also through easily executable cyber-attacks. This sudden awakening created a paradigm shift in the prioritization of homeland cybersecurity and importance of educating the Korean public on cybersecurity.

South Korea recognizes that cyber-security is a matter of national security. The frequency and gravity of cyber-attacks have prompted the South Korean government to re-evaluate its cyber-security strategy. There are three agencies equipped to handle issues of cyber-security: The National Cyber-Security Center,

the Korea Internet and Security Agency (KISA), and the National Police Agency's Cyber Terror Response Center. These agencies are responsible for identifying, preventing, and responding to cyber-attacks and security threats.

Korea Internet and Security Agency (KISA):

KISA is committed to improving the competitiveness, reliability and security of Internet information and knowledge in Korea. The establishment date is 27 July 2009.

KISA establishes guiding policies to a safe Internet environment and Internet infrastructure. They develop policies to advance and improve Internet security by envisioning the future of the Internet and analyzing potential threats. In addition, we are devoted to reorganizing related legislations to improve Internet culture and train professionals who can be a great help to lift the overall competency of national information protection.

9. TURKEY:

Turkey, in recent years, has been exposed to too many cyber-attacksfrom the country and abroad. Hacker groups have made attacks in Turkey,especially on public web pages. Attacks aregenerally performedto block the services as DDos: Distributed Denial of Service. Although

these attacks harbored political tendencies,they prevented the use of various citizenship services and disturbed individuals' work in daily life.

Cyber Security Board:

This Board was established with the verdict of the Council of Ministers in 2012. The administration, management, and coordination of national cyber security activities belong to this Board.

Intervention to National Cyber Events (USOM):

There are teams named SOME under the Intervention to National Cyber Events. SOME stands for Cyber Events Response Teams. They provide the necessary technical advice and assistance before the cyber events and, if necessary, alert the organization or institution. They give support during and after the cyber event. In all studies, they propose technical and administrative measures.

10. Italy

Italy updated its security laws in 2007 and adopted cybersecurity plans in 2013 and 2014, resulting in a strong legal framework supporting cybersecurity. The Italian cybersecurity strategy also calls out

public-private partnerships as the intended direction for cybersecurity, but no formalized cooperation yet exists. Its cybersecurity framework was published in February 2016.

Joint Cybernetic Operations Command (CIOC):

The Joint Cybernetic Operations Command has tasks in the areas of information security, computer network operations, cyber warfare and cyber security. It is designed to be a force provider.

According to CIOC Commander, Air Brigade General Francesco Vestito, the Command has two operational focus: cyber-defense and cyber network-defense. The cyber defense is related to the static defense and protection of the network, carried out in cooperation with the rest Italian military, in order to ensure the integrity of the network and the availability of the data flows. The cyber network-defense is related to the ability to carry out the vulnerability assessment and penetration test, in order to provide a quick intervention.

MUST KNOWN EVENTS

A. APPLE:

I. Data Private Fıght Between USA and APPLE:

For many years, Apple has used encryption to protect its customers' personal data because Apple believes it's the only way to keep information of customers safe. Apple has even put that data out of its own reach because apple believes the contents of your iPhone are none of its business. However, The United States government has been trying to force Apple to help investigators gain access to iPhones and asked a court to order Apple to create a unique version of iOS that would bypass security protections on the iPhone Lock screen.

Apple's CEO Tim Cook is not willing to cooperate with the government when it comes to allowing the organization a backdoor to its encryption process that protects customers' personal information. Apple built strong security into the iPhone because people carry so much personal information on their phones today, and there are new data breaches every week affecting individuals, companies, and governments. The passcode lock and requirement for manual entry of the passcode are at the heart of the safeguards apple has built into iOS. It would be wrong to intentionally weaken their products with a government-ordered backdoor. If Apple loses control of data, they put both privacy and safety at risk.

II. Siri Is Always Listening:

According to information from sources, the company makes some of the recordings listen to the editors in order to understand Siri's behavior. Normally, Siri is activated with certain scripts, but it can also be heard for reasons such as the sound of a zipper or the incidentally lifting up the Apple Watch. In this case,

the user does not know. In particular, HomePod and Apple Watch devices cause false listening is expressed.

According to the British daily, “there have been countless instances of recordings featuring private discussions between doctors and patients, business deals, seemingly criminal dealings, sexual encounters and so on. These recordings are accompanied by user data showing location, contact details, and app data.”

B. Chinese-Authored Spyware Found on More Than 700 Million Android Phones:

More than 700 million Android smartphones, some of which were used in the U.S., carried hidden software that enabled surveillance by tracking user’s movements and communications, a Virginia-based team of security researchers found.

The firmware, discovered by Kryptowire, was reportedly authored by Chinese startup Shanghai Adups Technology Company. It was largely discovered on disposable and prepaid phones made overseas. An undisclosed Chinese manufacturing company is believed to have paid for Adups’ work.

The researchers discovered that Adups’ firmware transmitted data packets to a Chinese server every 72 hours. These packets contained user’s call logs, text messages, contact lists, GPS location, and other data.

According to the Chinese startups’ official website, Adups’ clients include two of China’s largest cellphone manufacturers: ZTE and Huawei.

C. HUAWEI:

For years Huawei has been beset by international legal issues. From accusations of intellectual property theft, to major international sanction violations, the company inarguably has a messy record of operating on the fringes of global law.

Huawei's 5G Equipment:

The United States is pushing its allies to shut out Chinese tech giant Huawei's 5G networks due to national security concerns as the high-speed technology is set to play a critical role in the 21st century, a Eurasia Group expert said Tuesday.

Japan, Washington's close ally, will reportedly stop buying Huawei and ZTE network equipment for government offices and its military forces. Huawei has also been excluded from providing technology for the core 5G network that's being developed by U.K. telecoms firm BT.

Australia and New Zealand have also banned Huawei from participating in building their 5G networks — the next generation of mobile technology expected to revolutionize the interaction of internet-connected devices and appliances.

The existing network through Turkey's serving two-thirds of Huawei, all Vodafone Turkey's infrastructure and Turk Telekom and Turkcell's infrastructure provides a very large portion.

Google quickly ended its business dealings with the Chinese company, meaning Huawei would have no early access to the Android ecosystem, ultimately locking its smartphones out of the Google Play Store and apps like Gmail and Maps. Intel, Broadcom and Qualcomm all reportedly ceased business with Huawei, cutting off the supply of hardware fundamental to several of the company's major products.

D. FACEBOOK

i. The Facebook–Cambridge Analytic Data Scandal:

The Facebook–Cambridge Analytic data scandal was a major political scandal in early 2018 when it was revealed that Cambridge Analytic had harvested the personal data of millions of peoples' Facebook profiles without their consent and used it for political advertising purposes. It has been described as a watershed moment in the public understanding of personal data and precipitated a massive fall in Facebook's stock price and calls for tighter regulation of tech companies' use of personal data.

Harry Davies, a journalist for The Guardian reported that Cambridge Analytic was working for the United States Senator Ted Cruz using data harvested from millions of people's Facebook accounts without their consent. Facebook refused to comment on the story other than to say it was investigating.

The three news organizations published simultaneously on March 17, 2018, and caused a huge public outcry. More than $100 billion was knocked off Facebook's market capitalization in days and politicians in the US and UK demanded answers from Facebook CEO Mark Zuckerberg. The scandal eventually led to him agreeing to testify in front of the United States Congress.

ii. Facebook Has Leaked 419 Million Phone Numbers:

According to TechCrunch, a total of 419 million users, mainly from the United States, Vietnam and the UK phone numbers leaked to the Internet because Facebook's server is not password-protected. The data included Facebook IDs and

in some cases names, genders, and countries. Because the server hosting the database wasn't password-protected, anyone could find and access it, according to Sanyam Jain, the researcher who passed his discovery on to TechCrunch. It's unclear who pulled the information from Facebook's systems or why, but presumably it must have been an employee to have that level of access.

The exposed server included 133 million records from US-based Facebook users and 18 million UK users. Another had over 50 million records from users in Vietnam.

E. Instagram Breach Exposes Personal Data of 49 Million Users:

Facebook took yet another blow last week when subsidiary site Instagram was breached, exposing the sensitive data of at least 49 million users. And the leak was caused by yet another unprotected Amazon Web Services (AWS) server connected to the internet, a trend that has ensnared a disturbing number of high-profile companies in recent years – including Facebook in a previous incident just last month.

The leak was discovered by security researcher Anurag Sen sometime in mid-May and published on May 20. The AWS database, which belonged to a Mumbai-based marketing company called Chtrbox, appears to have been online without a password for at least 72 hours. Roughly 1 out of 20 Instagram users was affected by this.

The exposed database contained the profile pictures, city and country location, phone number, email address and the number of followers of each user.

F. GOOGLE:

a. Google +:

Google has pushed forward the shutdown of its failed Google+ social network following the discovery of a major data breach that exposed personal data of 52.2 million users. The bug prompted Google to announce that Google+ would officially shut down on August 2019, however, this has now been expedited to April.

Google Outs Indian Man to Authorities:

An Indian man was arrested over the weekend for allegedly posting derogatory and vulgar content about Indian politician Sonia Gandhi on Google's social networking site, Orkut. 22-year-old Rahul Krishnakumar Vaid had posted his comments in an Orkut community called "I hate Sonia Gandhi" through an Orkut account associated with his Gmail account. With Google's help, local authorities were able to verify Vaid's identity and make the arrest.

b. Don’t Trust Google Maps for Banks’ Contact Details:

Scammers are now increasingly interested in defrauding users through Google Maps that lets users change or correct the listings displayed on the service. Seeing this as an effectively exploitable opportunity, scammers are modifying the contact information of banks on the app’s listings.

This is a wicked tactic without even performing any complex tricks or using advanced tools fraudsters can trap innocent bank customers. Since the contact details have been updated by scammers, bank customers will call them instead of

the bank's official customer service. This way, scammers can easily extract sensitive banking data that use it to steal money from the victims' accounts.

A warning has been put out by Maharashtra, India, police regarding the new scam. The police, reportedly, received multiple complaints in the past month in which bank customers had to go through such a traumatic experience. However, the warning applies to Indian scammers only and not on cybercriminals in other parts of the world trying to benefit from Google Maps. So far, Google hasn't issued a statement in response to the news of the scam scammers are now increasingly interested in defrauding users through Google Maps that lets users change or correct the listings displayed on the service. Seeing this as an effectively exploitable opportunity, scammers are modifying the contact information of banks on the app's listings.

G. WINDOWS:

In 1997, researcher Aaron Spangler discovered a bug in Internet Explorer that allowed an attacker to steal credentials using a protocol known as Windows Server Message Block (SMB). Eighteen years later, a researcher on the Cylance SPEAR research team testing a messaging app with that bug in mind discovered a much larger vulnerability that affects at least 31 applications including Adobe Reader, iTunes, Box, and Symantec SYMC Norton Security Scan on all versions of Windows. This new vulnerability, called "Redirect to SMB," allows user login credentials to be leaked from a variety of Windows applications by tricking the apps into authenticating with a rogue server. Redirect to SMB allows hackers to execute a man-in-the-middle attack on a Windows device, sending

communications to a malicious SMB server, which can then produce the user's username and encrypted password. After that, an attacker can decrypt the password and gain access to a variety of vulnerable applications. Cylance refers to it as a “forever-day” vulnerability, because the original bug has been an ongoing threat since its discovery in 1997. While Spangler's bug was limited to Internet Explorer, the Redirect to SMB vulnerability affects a number of applications on all versions of Windows.

H. Smart TVs Sending Private Data to Netflix, Google and Facebook:

The smart TVs in our homes are leaking sensitive user data to companies including Netflix, Google and Facebook even when some devices are idle, according to two large-scale analyses.

Researchers from Northeastern University in the US and Imperial College London found that a number of smart TVs, including those made by Samsung and LG, and the streaming dongles Roku and Amazon’s Fire TV, were sending out data such as location and IP address to Netflix and third-party advertisers. The data was being sent whether or not the user had a Netflix account. The researchers also found that other smart devices including speakers and cameras were sending user data to dozens of third parties including Spotify and Microsoft.

REFERENCES

1. https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf
2. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
3. https://tweaklibrary.com/40-cyber-security-terms-you-should-be-knowing/
4. http://eweb.cabq.gov/CyberSecurity/Additional%20Security%20Documents/Reporting%20a%20Cyber%20Security%20incident.pdf
5. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf
6. http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-e.pdf
7. https://www.ppc.go.jp/en/aboutus/roles/
8. https://www.lexology.com/library/detail.aspx?g=1e0a8e7a-5347-4b55-bcb5-0765d90f4419
9. https://www.technologyreview.com/f/614268/facebook-has-leaked-419-million-phone-numbers/
10. https://www.forbes.com/sites/jeanbaptiste/2019/07/30/confirmed-apple-caught-in-siri-privacy-scandal-let-contractors-listen-to-private-voice-recordings/#509b25777314https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-plus-shut-down-date-bug-personal-data-breach-alphabet-inc-a8677296.html
11. https://arstechnica.com/tech-policy/2008/05/maybe-a-little-evil-google-outs-indian-man-to-authorities/
12. https://www.hackread.com/fraudsters-changing-contact-details-of-bank-on-google-maps/
13. https://www.cpomagazine.com/cyber-security/instagram-breach-exposes-personal-data-of-49-million-users/
14. https://www.forbes.com/sites/katevinton/2015/04/13/18-year-old-security-flaw-allows-hackers-to-steal-credentials-from-all-versions-of-windows/#174896c83a7d
15. https://www.cnbc.com/2018/12/11/us-has-a-concerted-strategy-to-push-allies-to-reject-huawei-eurasia.html
16. https://newatlas.com/huawei-ban-us-what-spy-evidence-exists/59772/
17. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf
18. https://www.cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/
19. https://www.export.gov/article?id=Korea-Cyber-Security
20. https://blogs.absolute.com/archive/south-korea-develops-cyber-security-strategy/
21. https://www.irishtimes.com/business/technology/smart-tvs-sending-private-data-to-netflix-google-and-facebook-1.4022833
22. https://www.btk.gov.tr/siber-guvenlik-kurulu