Research Report - Data

Forum: Disarmament & International Security

Issue: Preventing the abuse of collected data as a weapon

Table of Contents:

INTRODUCTION:

In our modern world, which is filled with technology and suffused with masses of online data, cybersecurity has become more important than ever before.
The personal data of millions of users is stored on servers all over the world and is one of the most valuable goods these days.
The first data breach happened in 2005 when more than one million credit card numbers were stolen. Since that time, numerous cyberattacks have occurred, resulting in the theft of data belonging to billions of users. The most recent instance pertains to the disclosure of confidential information from Israel's nuclear facility by Iranian hackers.

The security of data is a major challenge nowadays and is now entertained as a topic of discussion in our committee in order to search for ways to prevent further misuse of data.

II. KEY TERMS

GDPR

The General Data Protection Regulation is a powerful regulation set into effect in 2018. It has more than 90 Articles covering a large amount of data safety, This regulation heavily fines any individual group or other that disobeys its agreed upon laws. These fines can get as high as 4 % of the gross product of the cybercriminal. Although more powerful in Europe, the GDPR is internationally recognized. Some of the GDPR's main principles are the minimization of data collection, the integrity and confidentiality of companies who collects data (with encryption etc.) and the accountability of ones' data not being shared or sold and many more. This is all to prevent any type of security breaches. Directly strengthening the cause of our topic.

Big Data

Big data, it is every piece of data collected on a person or group. Big data is collected from emails watched videos made posts and so on. This data too large to individually store, it is stored across machines with distribution systems such as "Hadoop distributed file system" it is split up across computers to ensure the safety of the files and insurance to not lose them. For instance, let's say a system, has a 400 megabyte file, it would be split into four 100mb parts which would be copied and split across many computers. So maybe one computes has files A and D the next B and C the next D and C and so on to insure the safety of these files.

Cyberattacks/warfare

Cyber warfare has been being used more and more as of recent. It is and has always been used to steal or destroy information from an opposing force. Cyberattacks can be done by anyone, including individuals, organizations, governments, and more. A nation being subject to a cyberattack could be in danger due to important documents or plans being stolen or leaked. But an individual could also receive a cyberattack, although uncommon. And the back and forth of cyberattacks is what cyber warfare is.

Digital citizenship

Digital Citizenship is the ability of individuals to use the internet in positive and constructive ways. But a digital citizen also has responsibilities, such as to communicate respectfully, not to

steal another individual's intellectual property, one of the responsibilities of a digital citizen is not to reveal data of others. If everyone was a perfect digital citizen, it would solve the issue of the weaponizations of stolen data. Ideally, Digital citizenship would make the internet a lot more constructive. It is generally an idea and is often not supported and not respected by many. There are many steps to digital citizenship, but there will always be someone who thinks they are above everyone and have the right to power over others.

IV. Timeline of key events

- Most Recent significant cyberattack
- March 2024

Iranian Hackers recently hacked into an Israeli nuclear facility and leaked sensitive files with the purpose of destroying its operating network.

- Signing of the GDPR
- May 2018

This was a massive leap in cybersecurity and prevention of data stealing due to the GDPR's tough regulations and even tougher fines. Just in 2023 the GDPR has imposed more than 2.1 billion Euros of fines, which is more than the previous three years combined.

- Yahoo Data Breach
- October 2017

In 2017 yahoo admitted that hackers had stolen accounts. This was no small hack, this was one of the largest to date. With 3 billion accounts being compromised by hackers and data being consistently stolen. After this, Yahoo made its users reset all their passwords.

- First data breach
- 2005

This was the First data breach ever, compromising more than 1 million credit card numbers. This was the first one, but it started a trend and in that same year there were more than 100 data breaches.

GENERAL OVERVIEW

In a digitalized world, an individual's, company's or even national data can be exploited and abuse of collected data can result in infringement on people's rights or leaking company secrets or even a country's database. Rigid cybersecurity measures need to be put in place to prevent such attacks or misuse.

So how can collected data undermine national security? Nation states, non state actors or other malicious organizations or individuals can conduct cyber espionage to gain sensitive government data, classified military information or other collected data to gain strategic advantages, compromise mational defense or disrupt a country's economy by attacking important infrastructure to gain something valuable from the country's government or to convey a message to its citizens. In 2015 a breach of the U.S. Office of Personnel Management (OPM), where personal information of millions of federal employees and security clearance applicants was compromised, possibly leaking confidential government data. The second possible outcome of cyberattacks is manipulation of the public opinion and even the outcomes of elections or other activities of a government. According to the Brennan Centre for Justice that in the USA "since 2016, we have seen continued cyberattacks against political campaigns tied to both Russia and Iran." And at least one major elections vendor was successfully breached. By analyzing personal data collected from for example social media, hackers can identify vulnerable members of a country's society and feed them with propaganda and fake news, possibly to push through some political agenda. A notable example is the Cambridge Analytica Scandal where millions of Facebook accounts' data was collected and used to influence for example the 2016 US presidential elections. Allegedly, Cambridge Analytica

provided the Republicans with hundreds of thousands of US Facebook users' personality traits which were used to develop targeted propaganda for one candidate.

Cyber attacks can, however, cause even bigger damage in terms of physical casualties. For example, the Stuxnet virus, discovered in 2010, was designed to sabotage Iran's nuclear program by targeting industrial control systems, which underlines just how vital cybersecurity is in terms of world peace. But not only can data breaches cause damage to military equipment and operations, it can attack city infrastructure like power grids or transportation networks.

What measures are already in place?

Everyone probably knows the infamous abbreviation GRPR, which stands for General Data Protection Regulation. It's a comprehensive data protection law implemented by the European Union (EU) in May 2018 aiming to give EU citizens more control over their personal data and reshape the way organizations approach data privacy. Its policy includes intelligible consent requirements for data collection, prohibits pre-checked boxes for data collecting third parties and informing a user within 72 hours of a data breach to prevent further exposure. It also provides one with the right to access, rectify and erase one's data within the EU.It sets strong regulations for organizations that handle private data and non-compliance results in hefty fines of either 20 million dollars or 4% of the company's global annual revenue, whichever one is higher.

Other international treaties, councils and policies include:

- United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security
- Convention on Cybercrime (Budapest Convention)
- European Union Agency for Cybersecurity (ENISA)

- Global Forum on Cyber Expertise (GFCE)
- The Paris Call for Trust and Security in Cyberspace

Another way to look at data as a weapon is when a citizen willingly provides an attacker or scammer with data which can include credit card numbers, social security numbers or photos which can be either used for exploiting one's financial resources, defamation or material for extortion. It is therefore necessary to not only implement safety measures for countries and organizations but to educate the population to prevent further spread of scams and therefore more harm. Cybersecurity is vital for a working digialized society and measures on all levels should be implemented to improve the privacy and confidentiality of valuable data.

Major parties:

USA:

The United States are one of the global leaders in technology and cybersecurity. Millions of companies are located in the US, operate from there and usually store their user data there as well. It has significant capabilities in cyber defence and intelligence gathering, making it a key player in countering cyber espionage and attacks.

China:

With its burgeoning technological prowess and extensive cyber capabilities, China is a major partie in the cyber security discussion. It has been implicated in various cyber espionage activities targeting government, commercial, and academic entities, thereby underscoring its significance in cybersecurity discourses.

Russia:

Russia is widely recognized for its sophisticated cyber capabilities and alleged involvement in state-sponsored cyber operations, making it a prominent player in the realm of cyber warfare and espionage. Its actions in cyberspace have raised concerns about the manipulation of public opinion, election interference, and destabilization efforts.

European Union:

The European Union, comprised of member states possessing diverse technological infrastructures and regulatory frameworks, plays a pivotal role in establishing standards for data protection and cybersecurity. Initiatives like the General Data Protection Regulation (GDPR) demonstrate the EU's commitment to safeguarding individuals' privacy rights and enhancing cybersecurity resilience.

DPRK:

The German Bundesamt für Verfassungsschutz (BfV) of the Federal Republic of Germany and the National Intelligence Service (NIS) of the Republic of Korea (ROK) issued a second Cyber Security Advisory (CSA) to raise awareness of cyber campaigns highly likely carried out by cyber actors of the DPRK.

They are targeting the defence sector, companies and research centres. The DPRK focuses on military strength and the theft of advanced defence technologies from targets around the world. The BfV and NIS reckon that the regime is using military technologies to modernize and improve the performance of conventional weapons and to develop new strategic weapon systems including ballistic missiles, reconnaissance satellites and submarines. DPRK increasingly uses cyber espionage as a cost-effective means to obtain military technologies.

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf

https://gdpr-info.eu/

https://gdpr.eu/what-is-gdpr/

https://hbr.org/2012/10/big-data-the-management-revolution

https://www.ibanet.org/Cyberattacks-as-war-crimes

https://www.coe.int/en/web/digital-citizenship-education/the-concept#:~:text=Digital%20citizens%20can%20be%20described,step%20with%20evolutions%20in%20society

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

.