DPSJMUN'18

GENERAL ASSEMBLY BACKGROUNDGUIDE

VASUDHADIXIT - Chairperson
ARJUN AHLUWALIA - Vice Chairperson
ANUSHKA GARG - Rapporteur

AGENDA:

Combating Threats of Cyber Warfare with special emphasis on Cambridge Analytics and Crypto Currency

LETTER FROM EXECUTIVE BOARD

DEAR DELEGATES,

It is an occasion of pride that the DPSJ MUN is on the cards once again. On behalf of the entire executive board, welcome to the “GENERAL ASSEMBLY” at DPSJ MUN 2018.

As for the committee, this year GA’s agenda looks to the future. We will be discussing new realm of warfare. Cyberspace is the new frontier for international warfare and non-state actors are the winning forces. In this warfare agenda, questions (of legality) arise because these attacks often cross the boundaries of national borders. More emphasis would be paid on “non state actors” acting in “cyber space”.

We strongly believe that good MUNners should go beyond hurling Reuter's reports or UN documents at each other and focus more on solutions, than allegations. The world needs more of that.

Right now, you are a group of high school students with a common interest in politics- In July, you will be transformed into government officials facing some of the most complex issues in our world today. Have fun with your role and leave your own beliefs behind for three days as you represent some of the most interesting and vocal diplomats in the world. We are very excited for the discussions and deliberations that will arise from this fantastic committee. We encourage each and every one of you to not only be diligent in your research and your professionalism during the conference, but also, most importantly, enjoy your time here in the company of many other talented, thoughtful, and amazing people.

Please feel free to reach out to us for any questions or your introduction at dgeneralassemblydpsj@gmail.com.
We look forward to meeting all of you in the fall! Until then, best wishes!

Executive Board

UN General Assembly

DPSJMUN 2018

INTRODUCTION

With the increasing proliferation of information and communication technologies (ICTs) and the growing opportunity for real-time borderless exchange, cyber security is a complex transnational issue that requires global cooperation for ensuring a safe Internet. Cybercrime has now become a business which exceeds a trillion dollars a year in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world, as well as countless businesses and the Governments of every nation. Cyberspace has become a virtual Wild West where nations can attack one another without necessarily inflicting physical damage and potentially without significant repercussions. The fact that cyber dependency has become so widespread in society, with complex interconnections between various sectors, has increased vulnerability to attacks against both civilian and military infrastructures. Cyber weapons—various malware denial-of-service tools, and so on—are used to monitor activities, extract information, and possibly even cripple enemy systems. Matters aren't exactly deescalating, either.

➢ Definition of key terms

Cyberface — the notional environment in which communication over computer networks occurs.

Cyber Warfare — a military action, carried out electronically, and not physically, where the weapon acts as information, and the tools are computers and the Internet. The task of this kind of war is to achieve certain goals in the economic, political, military, and other fields, by influencing society and the authorities with carefully prepared information.

The Internet — any set of computer networks that communicate using the Internet Protocol.

Cyberattack — a type of threat where immediate damage or disruption caused are the main concern.

Cyber Espionage — a type of threat which can provide the information needed to make a successful cyberattack or scandal and launch information warfare

Malware — malware, or malicious software, is any program or file that is harmful to a computer user. Malware includes computer viruses, worms, Trojan horses, and spyware. These malicious programs can perform a variety of functions, including stealing, encrypting, or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission.

Digital currency – electronic money used as an alternative or additional currency.

Crypto currency – form of digital currency created and controlled via using cryptographic methods.

Peer-to-peer transactions – electronic money transfers made from one person to another through an intermediary, typically referred to as a P2P payment application.

Mining – the process of adding transaction records to Bitcoin's public ledger of past transactions.

➢ Types of threat

Espionage

Traditional espionage is not an act of war, nor is cyber-espionage,[and both are generally assumed to be ongoing between major powers. Despite this assumption, some incidents can cause serious tensions between nations, and are often described as "attacks". For example:

- Massive spying by the US on many countries, revealed by Edward Snowden.
- After the NSA's spying on Germany's Chancellor Angela Merkel was revealed, the Chancellor compared the NSA with the Stasi.
- The NSA recording nearly every cell phone conversation in the Bahamas, without the Bahamian government's permission, and similar programs in Kenya, the Philippines, Mexico and Afghanistan.
- The "Titan Rain" probes of American defense contractors computer systems since 2003.
- The Office of Personnel Management data breach, in the US, widely attributed to China

Sabotage

Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment. Compromise of military systems, such as C4ISTAR components that are responsible for orders and communications could lead to their interception or malicious replacement. Power, water, fuel, communications, and transportation infrastructure all may be vulnerable to disruption.

In mid July 2010, security experts discovered a malicious software program called Stuxnet that had infiltrated factory computers and had spread to plants around the world. It is considered "the first attack on critical industrial infrastructure that sits at the foundation of modern economies," notes *The New York Times.*

Stuxnet, while extremely effective in delaying Iran's nuclear program for the development of nuclear weaponry, came at a high cost. For the first time, it became clear that not only could cyber weapons be defensive but they could be offensive. The large decentralization and scale of cyberspace makes it extremely difficult to direct from a policy perspective. Non-state actors can play as large a part in the cyber war space as state actors, which leads to dangerous, sometimes disastrous, consequences. Small groups of highly skilled malware developers are able to as effectively impact global politics and cyber warfare as large governmental agencies. A major aspect of this ability lies in the willingness of these groups to share their exploits and developments on the web as a form of arms proliferation. This allows lesser hackers to become more proficient in creating the large scale attacks that once only a small handful was skillful enough to manage. In addition, thriving black markets for these kinds of cyber weapons are buying and selling these cyber capabilities to the highest bidder without regard for consequences.

Denial-of-service attack

In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS attacks may not be limited to computer-based methods, as strategic physical attacks against infrastructure can be just as devastating.

Propaganda

Cyber propaganda is an effort to control information in whatever form it takes, and influence public opinion .It is a form of psychological warfare, except it uses social media, fake news websites and other digital means. In 2018, Sir Nicholas Carter, Chief of the General Staff of the British Army stated that this kind of attack from actors such as Russia "is a form of system warfare that seeks to de-legitimise the political and social system on which our military strength is based".[

“Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behavior to achieve a response that furthers the desired intent of the propagandist" Terrorist organizations can use this medium to brainwash people. It has been suggested that restricted media coverage of terrorist attacks would in turn decrease the amount of terrorist attacks that occur afterwards.

➢ Who are the cyber war superpowers?

The announcement by the United States that it is using its military Cyber Command to mount computer network attacks against Islamic State is a demonstration of how significant this new battle front has become. The United States is just one of many countries that have invested significant amounts of money in developing not just defences against attack, but the ability to mount damaging cyber warfare offensives .The countries which are believed to have the most developed cyber warfare capabilities are the United States, China, Russia, Israel and the United Kingdom.

The United States stepped up its focus on cyber warfare in 2010 when US Cyber Command brought together the cyber capabilities of the Army, Air Force, Navy and Marines under one roof.

China has followed a similar path, recently announcing it was unifying its capabilities to better develop its cyber warfare might.

Russia is also known to have heavyweight cyber capabilities. The country is strongly believed to have used cyber weapons to attack Georgia during the military incursion into the country in 2008. In early 2014, the Cyber Snake program that attacked the Ukraine is believed to be of Russian origin.

Israel’s emergence as a cyber-powerhouse – with an estimated 10% of global sales of computer and network security technology – has meant it is well placed as a cyberwar superpower.

And in Europe, London is seen as the centre of cyberwar specialism with the British government having invested heavily in cyber capabilities over recent years.

North Korea is believed to be behind a significant number of attacks on the United States including the one which recently targeted Sony.

Iran is rapidly developing its cyber capabilities and is thought to be behind several major attacks in the region.

➢ Notable Instances of Cyber attacks

France

France has been a notable target for Russian cyberwarfare in recent years. In 2015, the Paris-based French broadcasting service TV5Monde was attacked by hackers who used malicious software to attack and destroy the network's systems and take all twelve of its channels off the air. The attack was initially claimed by a group calling themselves the "Cyber Caliphate" however a more in-depth investigation by French authorities revealed the attack on the network had links to APT28, a GRU-affiliated hacker group. In May 2017, on the eve of the French presidential election, more than 20,000 e-mails belonging to the campaign of Emmanuel Macron were dumped on an anonymous file-sharing website, shortly after the campaign announced they had been hacked. Word of the leak spread rapidly through the Internet, facilitated by bots and spam accounts. An analysis by Flashpoint, an American cybersecurity firm, determined with "moderate confidence" that APT28 was the group behind the hacking and subsequent leak.

United Kingdom "Brexit" referendum

In the run up to the referendum on the United Kingdom exiting the European Union ("Brexit"), Prime Minister David Cameron suggested that Russia "might be happy" with a positive Brexit vote, while the Remain campaign accused the Kremlin of secretly backing a positive Brexit vote. In December 2016, Ben Bradshaw MP claimed in Parliament that Russia had interfered in the Brexit referendum campaign In February 2017, Bradshaw called on the British intelligence service, Government Communications Headquarters, currently under Boris Johnson as Foreign Secretary, to reveal the information it had on Russian interference In April 2017, the House of Commons Public Administration and Constitutional Affairs Select Committee issued a report stating, in regard to the June 2016 collapse of the government's voter registration website less than two hours prior to the originally scheduled registration deadline (which was then extended), that "the crash had indications of being a DDOS 'attack.'" The report also stated that there was "no direct evidence" supporting "these allegations about foreign interference." A Cabinet Office spokeswoman responded to the report: "We have been very clear about the cause of the website outage in June 2016. It was due to a spike in users just before the registration deadline. There is no evidence to suggest malign intervention." In June 2017, it was reported by *The Guardian* that "Leave" campaigner Nigel Farage was a "person of interest" in the United States Federal Bureau of Investigation into Russian interference in the United States 2016 Presidential election. In October 2017, Members of Parliament in the Culture, Media and Sport Committee demanded that Facebook, Twitter, Google and other social media corporations, to disclose all adverts and details of payments by Russia in the Brexit campaign.

➢ An Essential Classification of Non-State Actors Operating in Cyberspace

Non-state actors active in cyberspace having the potential to employ digital force or, to various degrees, to be involved in cyber military operations may substantially differ according to size, internal structure, motivational grounds, and relation with the state. Their size may vary from simple (even “unicellular”) organisms to large transnational groups. Their organizational structure may be informal, lacking a chain of command, or complex, formal, and stably hierarchical. They may be driven by economic, political, ideological, or religious motivations. Usually, such organisms do not pursue purely military goals, such as power-outcome, typical of state actors or traditional non-state groups that engage in kinetic warfare. Further, they may be directed or stimulated by states or be fiercely opposed to any connection with state political entities.

Criminal organizations: Due to the lucrative potential of cybercrime, criminal organizations have flourished in cyberspace. Criminal consortia with a presence or ramifications online are among the non-state actors operating in cyberspace that present a higher degree of structural formality and aptitude to interconnect with, the state. Their digital manifestations likely reflect the structured, hierarchical organization typical of the crime syndicates. The exclusively financial interest that fuels the organization is the focal point that permits its usability by the state, expressed through an economic relationship. Indeed, such organizations may prove to be ruthless enough and possess the necessary technology, knowledge, and structure to be effective in a cyber scenario. For instance, the Russian Business Network, a criminal organization which administers various illegal activities related to computer crimes—such as child pornography, phishing, spam, and malware distribution—appears, according to some commentators, to have contributed to the cyber attacks conducted in 2008 during the Russia–Georgia war and against Kyrgyzstan in 2009.

Hacktivists: Digital activist (or "hacktivists," a portmanteau of hackers and activists) groups are independent, politically or ideologically driven hacker groups. They may range from local units composed of no more than a dozen persons to large transnational organisms with several satellite sub-groups. .Their internal structure, essentially informal, is shaped by the virtual composition and social life of the group. Operations are usually planned and organized on digital platforms, such as fora or IRC channels. Given their activists nature, their actions are mainly driven by ideological and political motivations. They stand as a consequence of the virtualization and internationalization of the urban square—understood as an agora for exchanging and developing political and cultural idea(l)s—and of political and economic power. At the edge of the new millennium the numbers of attacks radically increased. Hacktivist groups are gradually extending their reach on every aspect of domestic and international politics that—according to their own view—expresses examples of injustice. This has let, and expectably will increasingly lead to, substantial participation of hacktivist groups in armed conflicts. In 2012, as a response to the Israeli military operation in Gaza Pillar of Defence, the hacktivist community Anonymous conducted a DDoS attack against several Israeli websites and posted online names, identification numbers, and personal emails of 5,000 Israeli Defence Force officials. In March 2014, it launched two operations (OpRussia and OpUkraine) striking Russian cyberspace with digital attacks in reaction to the Russian maneuvers in Crimea. Thus far, digital activists have mainly performed low-level demonstrative actions, primarily operating web defacements and denial of service attacks. Still, in a prospective view, these types of attacks are progressively acquiring dangerousness as the technology evolves (e.g., new species of DDOS attacks, SQL injections, or "recombinant DNA" malwares), becomes cheaper and more easily available and the state infrastructure reliance on technology grows, also geographically.

Patriotic hackers: Patriotic hacker groups present strong similarities—principally structural—to hacktivist groups. They are permanently or extemporaneously created (usually in the aftermath of precise events) hacker groups, exclusively driven by a patriotic devotion to defend the interests of their country. Such a strong ideological linkage with the state may translate to a relationship of control by state authorities, and usually carves their social form within national borders. Furthermore, when the patriotic motivations are linked with geopolitical claims based on religion, such hacker collectives may have connections with terrorist groups. Their actions are triggered by events that, according to their sensitivity, may damage the interests of, or pose a threat to, their country. For instance, cyber attacks against Estonian government websites and banks, in 2007 (which, inter alia, interfered with the telephone access to emergency services) were triggered by the Estonian government's decision to relocate a monument of the Soviet Era. The involvement of the Russian government was never proved; however, the attack was in all likelihood conducted by patriotic groups of hackers. The assistant of a Russian State Duma deputy and prominent member of the Nashi—a Russian youth political organization with digital protractions, strongly linked with the Russian government—openly admitted to having participated in the attack. A year later, following the enactment of a Lithuanian law banning the display of Soviet emblems, groups of patriotic hackers attacked Lithuanian websites and diffused online a “Hackers United against External Threats to Russia” manifesto. Russian hackers may have been implicated in numerous other cyber incidents. Active patriotic hacker groups may also be observed in other countries. Among them, Chinese patriotic hacker groups, such as the Red Hacker Alliance, are particularly active since the late 1990s.

➢ Notable instances of cyber attack by non state entities

Recruitment for AL-QAEDA and ISIS

Al-QAEDA was first to implement online terrorist activity in the form of propaganda, military instructions, videos and other informational videos. This considered a form of low intensity military effort, referred to as “Net War.” Notably, these materials are translated into multiple languages to reach a larger audience. Extremist groups have used platform such as blogs, messages, boards and email as sourced for quick dispersion of materials and indoctrination, with some groups even creating “social media like hubs for extremists” intent on becoming the next generation of terrorists, hijackers and even suicide bombers, these hubs generally known as bedroom jihad. AL-Qaeda is better in communicating its massages on the internet with its speed, agility and cultural relevance. A key strategy is to spend as much time with, and listen carefully to, a prospective recruit to understand their life and “share his joys and sadness.” Recruiters also instill the basic of Islam, but not mention jihad so not to appear too radical.

Today, the terrorist group ISIS initiates a large portion of online recruiting. The young teenage girls leaving their homes to become the bride of extremist, they are a target due to their impressionable age. The majority of these interactions occur online on websites such as Twitter. Recruiters will spend hours with prospective recruits in order to connect with them on a personal level, to understand their current life style, and then try to insert extremist beliefs into their daily life. MubinShaikh, a former recruiter for an extremist Islamic group, explained “We look for people who are isolated,” he said. “And if they are not isolated already, then we isolated them.” This makes full conversion to extremist beliefs faster and easier. Recruiters also will send packages with gifts to aid in their conversion, including chocolates and cards. For ISIS, social media is not only a recruiting mechanism, but also a method of “cheerleading for attacks without engaging in secret training.” ISIS deft use of social media caught the world off guard. ISIS wasn’t the first global terrorist group to come of the age in the internet era, but it was first to so effectively harness its power. ISIS has proved fluent in You Tube, Twitter, Instagram, Tumblr, internet memes and other social media. It took some time, but tech companies have finally taken a more aggressive and effective approach, spread headed by Twitter, which has pulled down more than 125,000 accounts for promoting terrorist activities in less than a year.

Amateur videos and images are also being uploaded daily by its foot-soldiers, which are then globally disseminated, both by ordinary users and mainstream news organizations hungry for images of a conflict their own cameras cannot access. The current geopolitical situation in the Middle East is depressingly familiar, but ISIS’s media sophistication is something new.

ISIS’s global media operation appears to have two key objectives; to provoke the US and its allies, and to recruit from outside the Middle East. Both seem to be working. In the former instance, the horrific videos of the beheadings of US journalists and aid workers have helped drag western power back into combat in the region. Meanwhile, the same countries have seen their citizens departs to join ISIS.

the Islamic State (ISIS) regularly puts glossy propaganda magazine aimed at recruiting jihadies from the west. it is sophisticated, slick, beautifully produced and printed in several language including English and it uploads the magazine online as an English-Language PDF and distributes it on social media.

Countries like the United States recognized a need to engage their enemy in regards to information sharing. in 2002 then-Secretary of Defence Donald Rumsfeld made efforts to establish the Office of Strategic Information. one mission of this office was to streamline the release of information to the media (with a goal of influencing foreign audience's perception of the United States). InSeptember 2014, US president Barak Obama led the UNSC in passing a resolution to limit the mobility of foreign fighters in an effort to specifically combat ISIS. the US propose the four-point strategy that they pushed to include in the resolution. First, it aimed to create new binding legal obligations for countries to expand on the original 2001 resolution, 1373.it called on them to prevent foreign fighters from crossing their boarders and asking them to rewrite their domestic law to join a terrorist group or sponsoring people with that goal as illegal.

➢ The Cambridge Analytica and the Facebook Scandal

It's a company that "uses data to change audience behavior," both commercially and politically, according to its website. Its London-based affiliate, SCL Group, has a history of dubious tricks in elections around the globe. Cambridge Analytica worked in support of the 2016 campaigns of Trump, Ted Cruz and Ben Carson, all Republicans. It was founded in 2013 by former Renaissance Technologies co-CEO Robert Mercer. Facebook is facing international investigations into the illicit harvesting of users' personal data. The information was collected by Cambridge Analytica, a political consulting firm that backed President Trump's 2016 election campaign.

According to a whistleblower, Cambridge Analytica gathered data from 50 million users (a figure that Facebook has now admitted could be as high as 87 million), then developed a software program that profiled these citizens to predict voting patterns – and, through micro-targeted ads, influence US citizens' voting decisions. Cambridge Analytica (CA) obtained voter data through a Facebook-linked app named 'thisisyourdigitallife'. Through the app, CA member AleksandrKogan paid Facebook users in exchange for a detailed personality test, supposedly for academic research purposes. the app also pulled personal data from all of the test-taker's linked Facebook friends without their consent—data that, per Face book's Platform Policy, can only be used to enhance the in-app experience, and should not be given out to anyone.

Instead, Kogan and his associates allegedly built a software platform for influencing US elections, and sold it to Donald Trump. In 2014, former Trump advisor Steve Bannon ran Cambridge Analytica.

Around a quarter of a million people took the test willingly, but millions of people reportedly had their private data used for political and financial gain without their knowledge or consent. The number of people affected was originally believed to be 50 million, but in a blog post on April 4, Facebook revised the figure to 87 million.

Facebook only became aware of CA’s breach of contract in 2016, but reportedly waited months to order CA to delete the data. The consulting firm subsequently ignored this order, and Facebook allegedly never followed up to check.

Only after the media asked for comment did Facebook apparently realize it had been duped for four years. Facebook responded by threatening to sue outlets reporting on the issue

➢ Cryptocurrency

It can be said that cryptocurrencies function is almost the same as cash because the only difference being there is their entirely virtual nature. On the one hand, these new currencies using peer-to-peer payment technology remove the long-time players from the equation. Central banks, mints, financial institutions and regulators, and established transaction networks such as SWIFT, NACHA and existing card platforms are out of the picture and are trying to find out how to adapt. On the other hand, the resulting environment is uncertain and risky. Nevertheless, there are no doubts that criminals have already adapted their attacks to include these platforms wherever and whenever the opportunity arises. Financial institutions need to remain vigilant and be agile to stay ahead of dishonest actors and ensure they remain relevant in an increasingly virtual, mobile and hyper-connected world. Cryptocurrencies like bitcoin have forever changed business and personal finance.

Major countries and organizations involved:

- The United States of America
- The European Union

• Bitcoin

Bitcoin is a Cryptocurrency and worldwide payment system. It is the first decentralized digitalCurrency, as the system works without a central bank or single administrator.

• SwiftCoin

Swift Coin is a Cryptocurrency using peer-to-peer, blockchain, proof-of-work, and encrypted mailapplication developed by Team Daniel Bruno since 2011. It is an appropriate alternative to Bitcointhat uses similar blockchain technology.

- Japan

• Dogecoin

Doge coin is a Cryptocurrency that uses an Internet meme as its logo. Introduced as a "joke currency"on 6 December 2013, Dogecoin quickly developed its own online community and reached aCapitalization of US$60 million in January 2014; as of December 2017, it has a capitalization of US$ 1 billion.

- World Bank

• Litecoin

Lite coin is a peer-to-peer Cryptocurrency and open source software project.

Creation and transfer of coins is based on an open source cryptographic protocol and is not managed by any central authority.

➢ Relevant treaties and UN resolutions:

- Council of Europe’s 2001 Budapest Convention on Cybercrime.

  UN Resolutions Related to Cybersecurity:

- Resolution 56/121, January 2002

  Combating the criminal misuse of information technologies

- Resolution 58/199, January 2004

  Creation of a global culture of cyber-security and the protection of critical information infrastructures

- Resolution 64/211, March 2010

  Creation of a global culture of cyber-security and taking stock of national efforts to protect critical

  information infrastructures

- Resolution 70/237, December 2015

  Developments in the field of information and telecommunications in the context of international security.

As far as Cryptocurrency is concerned, In 2016 the United Nations Research Institute for Social Development has published a 25-sheet review of the possible role that the Cryptocurrency can pay in building social and solidarity finance. According to the review, it is liable that within two or 6 three following decades the cryptocurrencies can be increasingly utilized as an alternative to the actual currency in numerous spheres, ranging from healthcare to the military expenses. The document also discusses the risks that are associated with cryptocurrencies and clearly explains all the basics. The UN is gradually embracing the block chain system, which is reported in the UN Desk Review from the August 2017.

➢ FEW QUESTIONS A RESOLUTION MUST ANSWER

- Should the nations reinterpret their cyber convention principles?
- Are cyber weapons analogous to weapons banned by the GENEVA PROTOCOL?
- Should there be a third “other-than-war “mode for cyberspace?
- Concepts for a generalized approach that supports situational awareness of the cyber battle space or “terrain”.
- Can a state that suffers a cyber attack assert a right of self-defense against the non-state actor with reference to Article 51 of the UN Charter/
- Can a attack committed by a non-state actor in cyberspace be termed an “armed attack”.

➢ Reliable and Useful Sources:

https://unoda-web.s3-accelerate.amazonaws.com/wpcontent/uploads/assets/HomePage/ODAPublications/OccasionalPapers/PDF/OP19.pdf

https://www.itu.int/en/action/cybersecurity/Pages/default.aspx

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

https://ccdcoe.org/publications/2012proceedings/2_3_Arimatsu_ATreatyForGoverningCyberWeapons.pdf

https://www.icrc.org/en/international-review/article/get-my-cloud-cyber-warfare-internationalhumanitarian-law-and

https://link.springer.com/article/10.1007/s13347-017-0271-5

http://www.darthtrade.com

https://lemon-in.com/

https://www.theguardian.com/technology/2018/feb/02/bitcoin-bananacoinprodeum-cryptocurrencies

https://www.cnbc.com/cryptocurrency/

https://coinranking.com/

http://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-price-latestvalue-cryptocurrency-plunge-bubble-live-updates-record-november-a8190931.html

https://finance.yahoo.com/cryptocurrencies/heatmap/