UNION OF STATE HACKERS

Authors: Tejas Wattamwar, Valeria Granada and Maria Jose Lizarazo

Time for Opening Speech: 90 seconds

DESCRIPTION OF THE COMMITTEE

The Union of State hackers is an international organization of hacker representatives, which works against any attempt or act of cyber disturbance that may affect intergovernmental or strategic affairs. This committee was created in 2013, 10 years after the insurgency of "Anonymous" the hacktivist organization, and one year after the Russian operation, where this organization broke down into qualified information of "pro-Klemin" (pro-government) officials. Since then, this committee has met annually to discuss current deficiencies, or acts of belligerency in the cyber world and possible actions to be taken by each country regarding the situation that threats international security.

TOPIC A: AVOIDING CYBERWARS

GLOSSARY

Cyberspace:

An international area of the information environment made up of independent networks of information technology infrastructures, such as the internet, telecommunication networks, computer systems, embedded processors and controllers.

Cyberspace operations:

Anything done in and through cyberspace to support the department of military, intelligence, and business operations.

Cyber warfare:

Effects in and through cyberspace are created to assist the military goals of the combatant commander, guarantee friendly forces freedom of operation there, and keep enemies out.

Cyber Attack:

Actions used in cyberwarfare were intended to alter or deny cyberspace infrastructure and/or information. Attacks from below are regarded as flames.

Cyber Defense:

Cyber warfare makes it possible for operations and intelligence gathering activities to look for, gather information from, identify, and find targets in cyberspace for the purpose of recognizing threats, making targets, planning, and carrying out future operations.

Cyber Exploitation:

Cyberwarfare allows for operations and intelligence gathering activities to look for, identify, and collect targets in cyberspace for threat recognition, targetting, planning, and carrying out future operations.

Cyber Warefare capability:

A skill or approach that combines hardware, software, and firmware to create an impact in cyberspace but has not been weaponized. All cyber tools are weapons or have the potential to be weapons:

Cyber weapon identification:

A cyber weapon's representation for inventory control based on the forensic characteristics of the weapon.

Deny:

To launch an attack that reduces, disrupts, or completely eliminates access to or performance of a specific function to a level expressed as a % of capacity. The goal of denial is to avoid and use resources negatively.

Degrade:

To limit the operation of a particular function or access to it to a level expressed as a percentage of its capability. Normally, the desired level of deterioration is stated.

Disrupt:

Deny access to or operation of a targeted function entirely but momentarily, as represented by a function over time. Disruption is a specific form of degradation where the level of degradation is chosen.

Destroy:

To fully, irrevocably, and permanently deny a target access to its operation. The denial effect known as destruction maximizes both time and level.

Misfire:

The failure of a weapon to perform as intended, the whole or partial failure of a primary propelling change, transmitter, emitter, computer, software, or other munitions component.

Direct effect:

A result that the weapon's operation immediately causes. called the first order effect as well

Indirect Effect:

A result that follows directly or indirectly from one or more direct impacts of the use of weapons. Additionally known as the second, third, and effects' order numbers

Atribution Risk:

The chance that the discovery of a weapon or its effects will make it possible to pinpoint the attack's origin, perpetrator, or source of weapons.

CONTEXT

Cyber warfare is one of the largest concerns humanity faces in modern times. This is evidenced, as the increase of technology begins possessing all the control within modern society. Technology has taken an essential position within society. Due to this, it must be controlled and moderated to all expenses.

Warfare, and cyber warfare have generated a notable increasement within time. Matters such as these ones, first came to the spotlight after September 11th, 2001, in the wake of the demolition regarding the twin towers. Cyberwarfare nowadays is considered a simple hack done by an individual on a computer to a governmental organization trying to leak other government's information. Cyberwar is so dangerous that it can destroy and demolish through certain codes complete nuclear bases and programs. This is evidenced within the computer virus named “Stuxnet”. Said virus, is responsible for tearning down a secret Iranian nuclear weapon’s base plant.

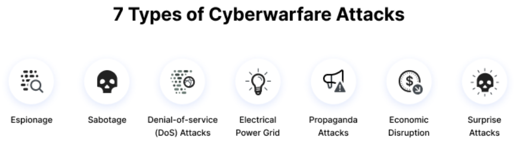
Within the evolution of technology, there are higher chances of being able to perform the act of ‘hacking’. The power of hacking can do unfixable damage to different aspects within society. To name a few, the perpetration of the economy, along with laboral-related matters. Notwithstanding, *hacking* is able to generate conflicts in the international community, where it arrives to the point that physical and tactile damages, make presence. There is a necessity for more regulation considering cyber warfare, as many existing forms of warfare agreements and treaties don't consider cyberwar, under their jurisdictions.

A cyberwar might easily develop into a real *war* with real casualties and actual weaponry. Despite the devastation that cyberwarfare may do, there are surprisingly few guidelines for how it should be fought, or better still, avoided.

Cyber Weapons are here to stay, and there is no stopping their proliferation. The world should instead adopt a set of principles to determine the proper behavior of countries with regard to cyberconflict, just as it has been done for other damaging technologies. They would establish guidelines for how to correctly attribute cyberattacks so that the certainty of the perpetrators' identities could be known, and for how nations ought to react. Perhaps most importantly, world leaders ought to establish a system of rewards and penalties that motivates nations to prevent harmful cyberattacks in the first place. A cyberwar might easily develop into a real war with real casualties and actual weaponry. Despite the devastation that cyberwarfare may do, there are surprisingly few guidelines for how it should be fought, or better still, avoided. A multilateral treaty would be ideal for enforcing these norms, but given the state of the international system and the reality that nations don't control all the tools of cyberwar, this strategy looks unworkable in the near future. However, progress towards more modest, concrete objectives, can be reached.

NATO members, for instance, may work together to improve detection and response methods by exchanging forensic information from cyberattacks. Separately, nations may form global working groups to talk about how to respond to attacks and what to do in the days or weeks before it can be discovered who or where they came from. Expecting one nation to unilaterally dismantle its cyberweapons while the risks are still present, is absurd. But when a nation is attacked online by another, governments may start debating what constitutes an acceptable response.

If not, it's just a matter of time before a country that has been *attacked* online replies by bombing the suspected attacker before the proof is clear. The world needs a legally binding treaty on cyberwarfare, and the United States is well positioned to lead this endeavor. Many of the organizations, notably research universities and the technology sector, that would be crucial in guiding these concepts are situated in the United States. Leading by example would be a crucial component of this campaign, and the United States can and should do precisely that. An effective system to control international behavior cannot be developed or run in secret; the process must be open. Governments avoid any public acknowledgement of their own capabilities and avoid engaging in any kind of "cyber diplomacy" because the majority of cyberwar is waged clandestinely. Secret diplomacy falls short of establishing deterrent public norms. It may seem difficult to coordinate such an attempt in our uncertain and tumultuous world environment. Governments have already hacked elections, stolen billions of dollars, damaged vital infrastructure, censored the press, manipulated public discourse on important subjects, and harassed journalists and dissidents using cyberweapons. Globally, cyberconflict is becoming more intense, and the instruments are becoming more affordable and accessible.



Types of Cyberware Attacks(This simple diagram shows the 7 most common types of cyberware and shows what is considered as cybererwarfare.) Source:Imperva

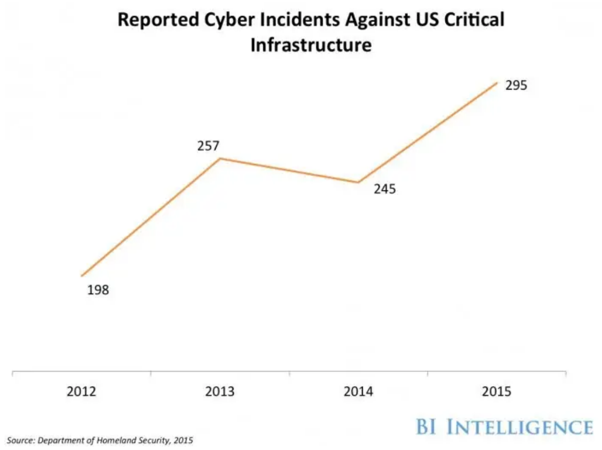
CAUSES

Cyberwars have had a sudden increase in the 21st century and in this short amount of time it is one of the largest threats to humanity as more and more government weapon systems.

As the world becomes more and more technological, there is an increase in cyberwars as hacking computers. As technological revolution of the 21st century is reached, warfare changes completely and new tactics were needed to coop up. Nowadays, the definition of cyberwars is vague each government and person may have a different definition of it, but the widely agreed definitions are that it is acts of espionage, sabotage, and denial of service attacks. Cyberattacks have created a whole new industry of security which is cybersecurity and as hackers get better and as information is more important than ever, hackers are always trying harder and harder to hack people to get their information. It can be said that the two main causes of the increase is cyberwars are the expansion in technology, its dependence and the inflation in the value of information.

REPERCUSSIONS

Nowadays, as Cyberattacks increase around the world and usually important documents and information is protected threw cybersecurity but in many instances, hackers have broken in having serious problems these are some of these events:



Source: Department of Homeland Security, 2015

May 2020-American Governmental Cyberattack and Leaks *(NSA discovered that Russian Attackers were robbing sensitive data from American governmental organizations through a popular email server)**Affected: United States Government***

June 2020- Cyberattacks against Indian Human Rights Activist Early in 2021, information emerged that a prominent government critic and imprisoned human rights activist had been the subject of hackers who had placed damaging material on his laptop prior to his detention on lawlessness-related charges. Now, a year later, a report by American specialists claims that the activist Rona Wilson was targeted by two distinct groups, including one group that has been connected to well-documented cyberespionage activities targeting military targets in China and Pakistan, India's two main international foes.

According to the report, the other group, called ModifiedElephant by SentinelOne, traded hacking tools with an attacker whose researchers have long suspected of engaging in state-sponsored political espionage. This group was in charge of placing documents on the activist's laptop. The information was revealed in a study by the cybersecurity company SentinelOne, which is based in California. It put light on what appeared to be a coordinated, almost ten-year campaign to monitor a group of dissidents. It also provides additional hints about the relationships between groups that cybersecurity experts have seen aiming their attacks at both domestic detractors and international foes.

The report makes note that ModifiedElephant's behavior "aligns with Indian state interests" but does not name the perpetrators of the attacks or the organization that gave the orders. Juan Andres Guerrero-Saade, a primary threat researcher and co-author of the SentinelOne study, noted that the fact that two distinct organizations were pursuing the same target shows that they were given the assignment by the same entity. SentinelOne researchers claim that Wilson received numerous emails with malware intended to penetrate his machine, many of which were sent by other activists he knew and occasionally passed off as news pieces. The Washington Post published an article in April about a different forensic investigation that revealed that years before Wilson's arrest, an unidentified hacker infiltrated his computer and planted at least 32 documents, including a letter outlining a plot to kill Prime Minister Narendra Modi that has been used as evidence against him by the authorities.

SentinelOne discovered that Hangover, a hacker collective, shared web domains with ModifiedElephant. SentinelOne's investigation was based on a 2013 report that revealed attacks by Hangover against commercial targets and national security targets in Pakistan, the United States, and Europe. Wilson was the second target of SideWinder, according to the SentinelOne investigation. SideWinder is well-known to international cybersecurity researchers who have followed its operations against military and governmental sites in Pakistan and China.

At the request of The Post, three impartial experts from the US and Europe analyzed the SentinelOne report and agreed with its conclusions. The new information suggests that Wilson, a 50-year-old human rights activist who is currently being held in a jail outside of Mumbai awaiting trial, was the victim of a protracted cyberattack campaign that involved multiple hackers and lasted for nearly ten years, a longer period of time than previously thought. The prosecution in the case, India's National Investigation Agency, did not respond to a request for comment. At a time when Modi's administration is defending itself against accusations of hacking and spying of its opponents, Wilson's case has caused controversy in India.

Numerous phone numbers from India were discovered to be on a global list of numbers chosen for surveillance by NSO Group's clients using its Pegasus program, which is exclusively licensed to government agencies, according to a global consortium investigation last year, which included The Post. On the list opposition party leaders, journalists, and activists from India, were included. The existence of the Indian government as a client of the NSO has not been confirmed or disputed. In December, Amnesty International reported that Wilson's iPhone 6s backup contained Pegasus malware evidence after being subjected to forensic examination.

Indian activists who were imprisoned on *terrorism-related* accusations were surveillance targets. In the Bhima Koregaon case, which started as an investigation into a violent confrontation between Hindu nationalists and Dalits, historically known as "untouchables," Wilson was detained in 2018 along with lawyers and academics. Wilson and 15 other people, were accused of having ties to a banned Maoist militant group by prosecutors, who charged them under a legislation against terrorism.

UN experts have urged the Modi administration to free the accused. One of the accused, an 84-year-old Jesuit priest, passed away in a hospital last July as a result of his condition deteriorating in custody. Wilson and his co-defendant, attorney Surendra Gadling, had their computers hacked last year, according to Arsenal Consulting, a Massachusetts-based digital forensics company, which discovered dozens of documents that were ultimately used as evidence by the prosecution. At the defense team's request, Arsenal examined their computers' electronic replicas while working for free. The findings are expanded upon in SentinelOne's report. Elephant, the main hacker, sent emails with documents or attachments that were customized to the victim's interests and were frequently copied to multiple recipients they knew, according to SentinelOne. These emails or attachments were laden with commercially available malware like NetWire and DarkComet. At least 32 emails from ModifiedElephant were sent to Wilson, and the group sent 40 emails to Gadling.

ModifiedElephant also targeted dozens of other civil society participants, including other co-defendants; it is unknown how many of these were infiltrated. Based on an examination of Arsenal's findings, malware infrastructure, and more than 100 *fishing* emails that Wilson and his co-defendants received, SentinelOne conducted their study. SentinelOne sought the defense team's emails and completed the assignment efficiently. The researchers claimed that the first attack on Wilson dates back to a decade ago, despite the fact that the email attacks grew more severe in 2014 and persisted at least until 2016. The *fishing* emails were linked to two separate organizations that simultaneously sent messages using free providers like Gmail and Yahoo. Along with ModifiedElephant, Wilson received at least four malicious emails from SideWinder between 2013 and 2014, a group that normally targets foreign targets and has been monitored for years by international researchers. The success of the SideWinder attacks is uncertain.

2019 saw the release of a warning from the Pakistani government describing attacks by SideWinder on its defense and government buildings, branding the perpetrators as Indians. By monitoring the Web domains connected to the emails, SentinelOne was able to distinguish between the two groups. A fresh revelation claims that further evidence in the case against Indian activists accused of terrorism was planted. Additionally, the investigation discovered evidence connecting ModifiedElephant to hangover. SentinelOne reported that at least two web domains used by ModifiedElephant to send phishing emails to Wilson were connected to Hangover, indicating a relationship between the two organizations. In 2013, Hangover was charged with targeting Norway's government-owned telecom operator. The most recent information about the campaign against Wilson, according to Snorre Fagerland, a Norwegian cybersecurity researcher who co-wrote a 2013 report on Hangover, helps to better understand the connections between attackers who may be operating in India and targeting both foreign adversaries and domestic dissidents.

June 2010-Stuxnet attack on Iranian Nuclear weapons factory

Summer 2010 saw the first appearance of the Stuxnet Worm. A 500 kilobyte computer worm called Stuxnet infected several computer systems. There were three steps taken by this pathogen. It started by scanning and focusing on Windows networks and computers. Once inside these devices, the worm started to multiply itself constantly. The machine then gained access to the Windows-based Siemens Step7 program. In industrial computing networks, such as those at nuclear enrichment facilities, this Siemens software system has been and still is widely used. The worm also got access to the industrial program logic controllers by compromising the Step7 software. This final phase enabled the worm's developers to operate a variety of machinery and gain access to vital industrial information.

The worm became so widespread due to the replicating technique that was previously mentioned. It was so pervasive that if a USB device was plugged into a machine that was infected, the worm would spread to any more computers that the USB was plugged into. The Stuxnet malware attacked and entered more than fifteen Iranian facilities. This attack is thought to have been started by a random employee's USB drive. The nuclear facility in Natanz was one among the industrial establishments that was impacted. The nuclear facility's computer system showed the first symptoms of a problem in 2010. When IAEA inspectors visited the Natanz facility, they saw that a strangely high percentage of Uranium enrichment centrifuges were breaking.

At the time, it was unclear what led to these errors. Later in 2010, Iranian technicians hired Belarusian computer security experts to audit their computer systems. Eventually, this security company located numerous harmful files on the Iranian computer systems. It was later discovered that the Stuxnet worm was contained in these malicious files. Iran hasn't provided detailed information on the attack's results, but the Stuxnet worm is thought to have destroyed 984 uranium-enrichment centrifuges as of right now. According to current estimates, this resulted in a 30% reduction in enrichment efficiency.

The creator of the Stuxnet worm and the individual(s) that employed it to essentially perpetrate Iran's nuclear plant, have both been the subject of much media speculation. Currently, it is accepted that this worm was created as a cyberweapon to target Iran's growing nuclear program. However, it is still uncertain who created the worm.

According to several experts, Israel and the United States collaborated to launch the Stuxnet worm strike against Iran's nuclear facilities. In 2013, NSA leaker Edward Snowden asserted that this was the situation. Despite these rumors, it is still unknown who actually created the first cyber weapon.

<u>July 2022- Ukrainian Broadcasting service Hacked</u>

On a Thursday, july 2022, two radio stations run by TAVR Media, one of the biggest broadcasters in Ukraine, were compromised in an attempt to spread false information about the hospitalization and grave condition of Volodymyr Zelensky. Melodia FM and Radio Bayraktar's music broadcasts were disrupted by hackers at around 1 p.m.. According to Oksana Shavel, a spokeswoman for the broadcaster, cybercriminals attempted to penetrate all nine radio stations, but the majority of the efforts were stopped by the company's cybersecurity team.

Hackers claimed in a bogus news story that Zelensky was in serious care and that the head of the Ukrainian parliament was in charge of carrying out his duties. Later on that day, Zelensky debunked the rumors in a video that was uploaded on his official Instagram profile. He declared, "I'm in my office and I'm healthier than ever." Zelensky has charged Russia with spreading false information, despite the fact that no group has yet claimed responsibility for the incident.

As the conflict in the field approaches the 150-day mark, the incident represents the most recent cyber tussle between Russian and Ukrainian hackers. Olexander Gluschenko, a Ukrainian telecom expert, told ‘The Record’ that people compete to see who can perform tasks more effectively. A pro-Ukrainian cyber gang assaulted a Russian radio station earlier in June so that it could play anti-war music and the country's anthem. Additionally, numerous Russian TV channels have frequently been hacked to broadcast live footage of the conflict in Ukraine.

The hacker group Anonymous gained access to the live TV networks Russia 24, Channel One, and Moscow 24 as well as the Russian streaming sites Wink and Ivi in order to broadcast conflict video from Ukraine. The attack against TAVR Media is still under investigation by Ukraine's CERT, and it is not yet obvious how the attackers gained access. One of the stations affected, Radio Bayraktar, began broadcasting nationalistic Ukrainian music in March of this year. The station is named after a Turkish drone that has come to represent Ukraine's struggle for independence. Shavel claims that the attack wasn't carefully prepared either. She remarked, "The message didn't seem like our typical news show. The hackers employed an artificial voice that made stylistic mistakes and talked in subpar Ukrainian.

Shavel continued, "We didn't even have time to feel confused; we blocked the communication right away. For roughly 30 seconds, a phony news report was broadcast. How many Ukrainians heard it remains unknown. This isn't the first time the Ukrainian media has been attacked. According to Cloudflare, online media, publishing, and broadcasting businesses were the subject of more distributed denial-of-service (DDoS) assaults in the second quarter of 2022 than any other sector.

Hackers targeted TAVR Media because its radio stations are the most listened to in the nation, Shavel claimed (independent ratings), therefore there is probably no meaning in the targets. A football game between Ukraine and Wales was broadcasted with Russian propaganda earlier in June after hackers attacked the Ukrainian streaming site Oll.tv. According to its general producer Dmytro Khorkin, Ukraine's national public broadcaster also experienced a DDoS attack in February. ''Since the start of the conflict in Ukraine, Russia has continuously attacked us'', he claimed to 'The Record'.

Both on the ground and online, Russian forces are attacking Ukraine's telecommunications infrastructure. According to Khorkin, eleven Ukrainian radio and television towers, as well as radio stations that broadcast to the occupied territory, have been damaged by Russian rockets since February 24.

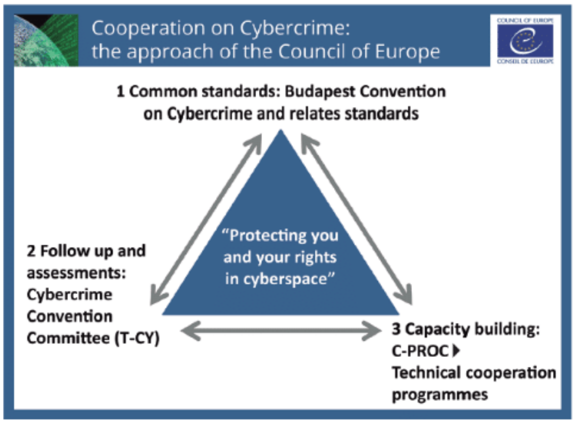
CURRENT SITUATION

International Actions

The topic of cyberwars and cybersecurity is a new and modern topic which involving by the day compared to many other topic's cybersecurity has fewer conventions and treaties relating to it especially one from organizations such as the UN but most important existing convention about the topic at the moment is:

The Budapest Convention of 23 November 2001 made by the countries in the Council of Europe

The Budapest convention is a convention signed by 50 countries which seek to increase cooperation between delegates to find possible solutions to cyberattacks and to maintain a policy of not attack the other countries in the resolution as well the treaty aims to improve inquires and the research process to fund the hackers and the countries involved in possible cyberattacks.



Cooperation on Cybercrime: the approach of the Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

"Protecting you and your rights in cyberspace"

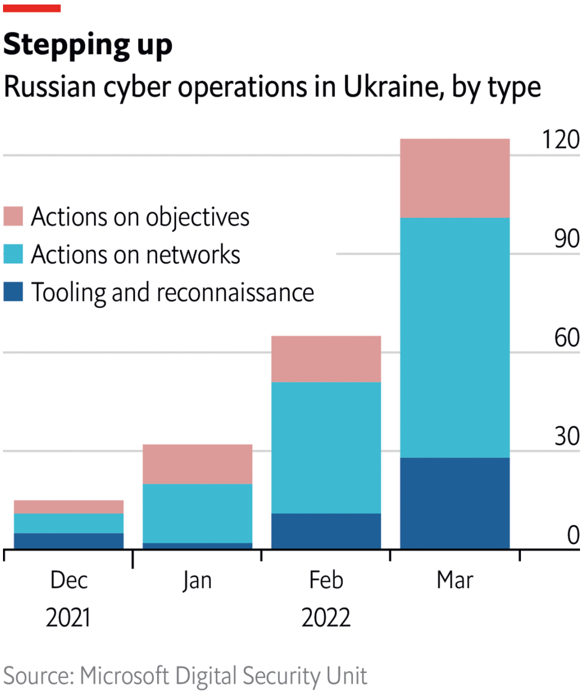
2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▸ Technical cooperation programmes

***Framework of** Budapest Convention on Cybercrime(This is a graph showing the triangle of the framework for the Budapest Convention on Cybercrime, and it shows as well how it operates) Source:Council of Europe*

Case study 1:Russian Cyberware in Estonia, and Ukraine

Throughout the years Russia has always been an outlier in cyberware, Russia is one of the countries which has the most cyberattacks on other countries and organizations. In 2007 Russia committed a cyberattack on Estonia where they robbed important documents and future plans of the Estonian government the Russian Government found plans of Estonia to create different trade agreements with western countries such as the United States of America and the United Kingdom after Russia found about this threat and Estonia by telling them if they continued with any of these plans then they would sever ties completely with Estonia. Russian cyberattacks on Ukraine from 2014-2017 lasted for a long period and consisted of flooding Ukrainian websites and media websites with Russian propaganda and destroying Ukrainian digital infrastructure, this was done to stop Ukraine to improve their relations with western countries as well it was done in rebellion against the new Ukrainian government.



Stepping up

Russian cyber operations in Ukraine, by type

Source: Microsoft Digital Security Unit

***December 2021-March 2022** (A report by the economist revels and shows the increase of cyberattacs by Russia towards Ukraine after the start of the war and the different recrupretions s in different fields of these attacks) Source:Economist*

After the start of the Russo-Ukraninan war, there was an increase in the cyberattacks from Russia towards Ukraine and these attacks are mainly strategic military attacks to jam communication or to display Russian propaganda in Ukraine.

Case study 2: Cyberattacks on Russia by the USA or France

As we have seen previously Russia has been charged of cyberattacks throughout the years, it is surprising to hear that in 2017

Russia was hacked and thousands of files were leaked including the property list of Vladimir Putin's private estate**s** as well as many details of the connection between the Russian oligarchs and President Vladimir Putin, Russian officials revealed a statement stating that they were investigating and bringing to justice to these hackers, many sources say that the responsible were USA governmental hackers but shortly after the attack on Russia, Russia launched a series of attacks on the presidential campaign of President Emmanuel Macron many consider this a counterattack and believe that this counterattack was done because Russia found evidence that the French government had hacked them, this was one of the many cyberwars Russia has fought over the years, this is one of the most recent ones and caused international headlines.

Case study 3 : United States of America's cyberwar with Iran

From 2009 till 2020 USA and Iran were in an ongoing cyberwar that was kept secret by both governments in this cyberwar there were multiple attacks from both sides, the public of both nations were heavily impacted and affected as both movements targeted personal devices of the public to spread different viruses, having the main goal of to reach governmental devices. The last confirmed cyberattack was from the USA where the objective was to collapse the foreign ministry in Tehran and not make new allies and expand their influence tensions rose to a huge level and the ambassadors of the USA and Iran sought out tensions and improved on their diplomatic relations. Most of the attacks from both sides were to find information about ongoing missions of the countries, this “invisible cyberwar” started in 2009 when Iran extended its cyberspace measures and technology and launched the first attack against the USA.

OBJECTIVES OF THE COMMITTEE

The Objective of the committee is to stop and create a popular legal basis to try to stop cyberwars the objective of the delegates will be to find available and long-term solutions and establish viable solutions which solve to an upcoming new form of war, delegates must think using different leadership and their creativity to find a solution which can function in any situation resulted to cyberwars, this solution should be effective as well the evaluation of how viable is cybersecurity should be taken into account.

GUIDING QUESTIONS

- Is your Country a victim or attacker in cyberspace?
- What position does your country held on cyberware?
- Does your country have rules and any treatise or agreements about cyberwar?
- Is your country highly technologically dependent?
- What is your Country's cybersecurity index on a global scale?
- What type of Cyberattacks are most common in your country?

SOURCES

- *Orr, T. (2018). A Brief History of Cyberwarfare | GRA Quantum. Retrieved 30 November 2022, from https://graquantum.com/a-brief-history-of-cyberwarfare/*
- What is Cyber Warfare | Types, Examples & Mitigation | Imperva. (2022). Retrieved 30 November 2022, from https://www.imperva.com/learn/application-security/cyber-warfare/
- (2022). Retrieved 30 November 2022, from https://www.youtube.com/watch?v=XbMUJpmSkxY
- Reasons behind cyber attacks | nibusinessinfo.co.uk. (2022). Retrieved 30 November 2022, from https://www.nib
- usinessinfo.co.uk/content/reasons-behind-cyber-attacks
- Cyberwarfare and Collateral Damages - GlobaLex. (2022). Retrieved 30 November 2022, from https://www.nyulawglobal.org/globalex/Cyberwarfare_Collateral_Damages.html
- Stuxnet Worm Attack on Iranian Nuclear Facilities. (2022). Retrieved 30 November 2022, from http://large.stanford.edu/courses/2015/ph241/holloway1/
- Ohanian, C., Ohanian, C., Bridgeman, T., Goodman, R., Gullo, K., & Schmon, C. et al. (2022). The UN Cybercrime Treaty Has a Cybersecurity Problem In It. Retrieved 30 November 2022, from https://www.justsecurity.org/83582/the-un-cybercrime-treaty-has-a-cybersecurity-problem-in-it/
- The Budapest Convention on Cybercrime: a framework for

capacity building – Global Forum on Cyber Expertise. (2022). Retrieved 30 November 2022, from https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/

- Cyber attacks against our critical infrastructure are likely to increase. (2022). Retrieved 30 November 2022, from https://www.businessinsider.com/cyber-attacks-against-our-critical-infrastructure-are-likely-to-increase-2016-5
- The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine from HACKS, LEAKS AND DISRUPTIONS:: RUSSIAN CYBER STRATEGIES on JSTOR . (2022). Retrieved 30 November 2022, from https://www.jstor.org/stable/resrep21140.9?seq=11#metadata_info_tab_contents
- Russia, This Time the Victim of a Cyberattack, Voices Outrage (Published 2017). (2017). Retrieved 30 November 2022, from https://www.nytimes.com/2017/05/14/world/europe/russia-cyberattack-wannacry-ransomware.html
- Russia seems to be co-ordinating cyber-attacks with its military campaign. (2022). Retrieved 30 November 2022, from https://www.economist.com/graphic-detail/2022/05/10/russia-seems-to-be-co-ordinating-cyber-attacks-with-its-military-campaign
- The Invisible U.S.-Iran Cyber War. (2019). Retrieved 30 November 2022, from https://iranprimer.usip.org/blog/2019/oct/25/invisible-us-iran-cyber-war

- **SUPPORT LINKS**
- Support Link 1
- Support Link 2
- Support Link 3
- Support Link 4
- Support Link 5

TOPIC B: DESTRIUCTION AND CAPTURE OF ANONYMOUS

CONTEXT

One of the most notorious hacker organizations in the world has gone by the name "Anonymous" for almost two decades. And the enigmatic internet group is once again in the news. Anonymous is a decentralized international organization and movement funded in 2003, that has been a collective movement of *"hacktivists"* (hacker-activists) in charge of attempting and making cyberattacks against governments, institutions, corporations, and intergovernmental agencies. Following Russia's invasion of Ukraine at the end of February, "Anonymous," a Twitter user with 7.9 million followers, declared a "cyber war" against Russia and its leader, Vladimir Putin.

Since then, the group has taken credit for a number of cyberattacks that have taken down websites and exposed information from Russian government institutions as well as state-run businesses and news organizations. Anonymous, also referred to as "hacktivist," performs coordinated assaults against various international governments, businesses, or other organizations, frequently in the name of social or political reasons. The "Anonymous" account, which states that it "cannot claim to speak for the whole of the Anonymous collective," urged hackers worldwide, including those in Russia, to say 'NO to Vladimir Putin's war," in a tweet on February 24.

In the early years of the website, users frequently planned "raids," in which they flooded chat rooms for games and other online communities to cause disturbances. After detractors charged participants with cyberbullying and publishing inappropriate material, 4chan started to crack down on the raids. These raids served as the inspiration for Anonymous, a decentralized group of like-minded internet users who planned online disruptions by communicating in encrypted chat rooms. Initially, the main focus of their programs was on low-cost entertainment. They eventually started to center on social or political objectives.

In 2008, 4chan users under the leadership of early Anonymous hacker Gregg Housh launched a coordinated attack against the Church of Scientology using tactics like denial-of-service (DDoS) attacks on the church's websites, sunt phone calls, and faxing the church's black pages to waste their printer ink. This was the group's most notable early example of "hacktivism." The hacker collective Anonymous called the attacks "Project Chanology," and they were in response to what they saw as an attempt at censorship: the church had threatened legal action against Gawker after the news site broadcast a hacked clip of star Tom Cruise gushing about Scientology.

A wave of anti-scientology protests across the globe quickly followed, with many Anonymous-supporting demonstrators donning masks of the 17th-century British insurrectionist Guy Fawkes. Since then, those masks have been intimately linked to a *hacking group.* Generally speaking, Anonymous is against censorship and inequality-promoting governments and businesses. There is frequently considerable internal disagreement about which ideas or causes to support because the group is disorganized and has any genuine hierarchy or structure.

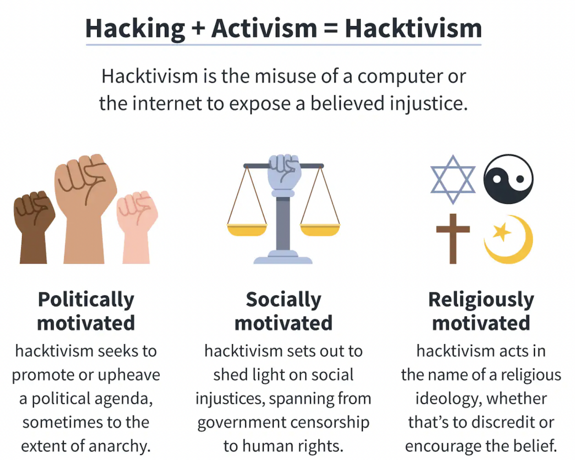
The @YourAnonNews Twitter account's pinned 2019 post, which once more asserts that it does not speak for the collective at large, characterizes Anonymous members as "working class folks wanting a better future for humanity." "Freedom of information, freedom of speech, accountability for businesses and governments, privacy and anonymity for private citizens" are listed as Anonymous' guiding values.

Since "Project Chanology," members of Anonymous have attacked a variety of targets, including: The Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA), after those groups sought to prevent websites that share copyrighted music and movies from operating. After federal authorities took down the file-sharing website Megaupload.com in 2012, the U.S. Department of Justice and FBI. PayPal, after the internet payment system stopped enabling contributions to Julian Assange, the contentious founder of WikiLeaks. Government websites were taken down in Tunisia, Egypt, and other Middle Eastern and African nations as a result of the 2011 Arab Spring pro-democracy demonstrations. ISIS, in the wake of the 2015 Paris attacks. Numerous suspected members of Anonymous have been detained by law enforcement agencies across the globe, including at least 14 individuals accused of hacking PayPal in 2011. Barrett Brown, a journalist and self-described spokesperson for Anonymous, was arrested in 2012 and sentenced to more than four years in jail after being accused of hacking and threatening a federal officer.

After some of those arrests, the group's activities slowed down, but they resumed last year when Anonymous took credit for hacking against the Texas Republican Party in opposition to the state's contentious abortion law. A hack of the web hosting provider Epik in September that resulted in the exposure of more than 150 terabytes of information about far-right organizations like QAnon and the Proud Boys was also attributed to Anonymous. One of the 100 Most Influential People in the World in 2012, according to Time magazine, was Anonymous. Millions of individuals now follow social media profiles connected to Anonymous.

Co-founder of the cybersecurity firm Security Discovery, Jeremiah Fowler,
told CNBC last week that the group's adherents probably saw Anonymous as a kind of "virtual Robin Hood," taking on strong corporations and governments in the name of progressive causes. According to Fowler, hacktivists and groups like Anonymous provide individuals with that immediate gratification. However, Anonymous does have detractors. The group's vigilante actions are viewed by many as extreme and potentially deadly. The National Security Agency classified Anonymous as a national security threat in 2012. Even the group's fans should take into account that the legacy of Anonymous is a mixed bag, according to writer Parmy Olson, who wrote a 415-page book about the organization in 2012.

"Has Anonymous improved the world in any way? Yes, sometimes," Olson said Radio Free Europe/Radio Liberty. Since the group is decentralized, it has no real structure or hierarchy hence it must be destroyed.



Hacking + Activism = Hacktivism

Hacktivism is the misuse of a computer or the internet to expose a believed injustice.

Politically motivated hacktivism seeks to promote or upheave a political agenda, sometimes to the extent of anarchy.

Socially motivated hacktivism sets out to shed light on social injustices, spanning from government censorship to human rights.

Religiously motivated hacktivism acts in the name of a religious ideology, whether that's to discredit or encourage the belief.

*Hacktivism: An overview plus high-profile groups and examples. (n.d.). Norton. Retrieved November 5, 2022,from*https://us.norton.com/blog/emerging-threats/hacktivism

CAUSES

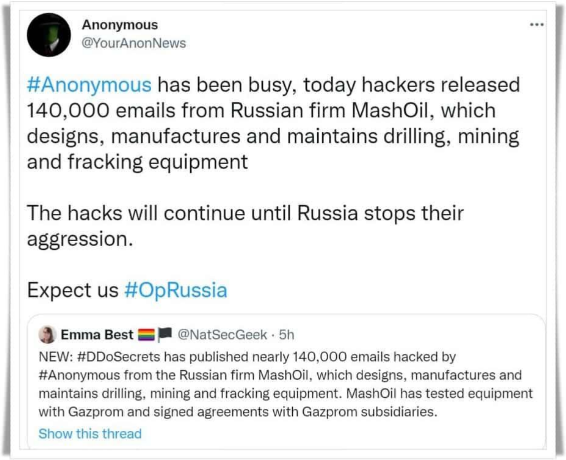
Anons is the term referring to the followers of the anonymous collective, which motive is to oppose mediatic censorship or control, most actions consist in targeting government, organizations, and corporation**s** belonging that are accused of mediatic manipulation/ censorship coming from "elites" of the mediatic media, or that promote inequalities. The insurgence of the

Anonymous collective has come due to international concerns about social or political deficiencies, following the legacy of *"We are anonymous, we are legion. We do not forgive and we do not forget".* Their symbol is a Guy Fawkes mask, from the novel "V for Vendetta", focused on an anarchist revolutionary who dons the mask to set a corrupt fascist government. Therefore, throughout the years, there have been multiple apparitions and attacks against political organizations or among different states and institutions.

REPERCUSSIONS

Authorities throughout the globe have detained several of suspected Anonymous ties, including at least 14 persons accused of breaching PayPal in 2011. Barrett Brown, self-proclaimed journalist and Anonymous representative was detained for more than four years after being arrested in 2012 on charges related to hacking and threatened federal agents in the United States.

After some of these arrests, the collective's activities decreased, but they reappeared last year (2021) when Anonymous claimed responsibility for hacking and targeting the Republican Party in Texas in protests of the government's controversial law regarding abortion. They also claimed responsibility for a breach of web-hosting company Epik, which resulted in the release of more than 150 gigabytes of data on far-right organizations like QAnon and the Proud Boys.



Anonymous
@YourAnonNews

#Anonymous has been busy, today hackers released 140,000 emails from Russian firm MashOil, which designs, manufactures and maintains drilling, mining and fracking equipment

The hacks will continue until Russia stops their aggression.

Expect us #OpRussia

Emma Best 🏳️‍🌈🏴 @NatSecGeek · 5h
NEW: #DDoSecrets has published nearly 140,000 emails hacked by #Anonymous from the Russian firm MashOil, which designs, manufactures and maintains drilling, mining and fracking equipment. MashOil has tested equipment with Gazprom and signed agreements with Gazprom subsidiaries.
Show this thread

Retrieved from:https://twitter.com/anonymous_co/status/1389497423366705155

CURRENT SITUATION

International Actions

Considering the anonymity of this entity, any judgment, sanction, or response to the attempts is uncertain. Any major action has been principally taken by the victims of the cyber attacks that anonymous has made, but has unsuccessfully developed due to the advanced operators that are behind this entity. Being so, there has been no significant action taken to the moment, despite statements against the accusations made by Anonymous, like it was with Donald Trump in 2018. Also, since anonymous has an unknown provenience or origins, it is impossible to directly accuse any country, organization or individual of responsibility for this entity or these crimes. Some of the most relevant events that involved the apparition of anonymous proceed the following:

2008 - Chronology Project

Project Chanology, also known as Operation Chanology, was an internet-based protest movement started by members of Anonymous against the activities of the Church of Scientology. 4chan and Scientology are combined to form "Chanology." In reaction to the Church of Scientology's efforts to get content from a well publicized interview with Scientologist Tom Cruise removed from the Internet in January 2008, the initiative was begun. On January 21, 2008, a video titled "Message to Scientology" was uploaded to YouTube and used to officially introduce the project

In the video, Anonymous claims that Scientology's tactics constitute Internet censorship and declares its intention to "expel the cult from the Internet." The Church of Scientology's operations were then targeted with distributed denial-of-service assaults (DDoS), which were quickly followed by prank calls, black faxes, and other disruptive tactics. The protest's focus switched to legal tactics in February 2008, including nonviolent demonstrations and an effort to get the Internal Revenue Service to look into the Church of Scientology's tax-exempt status in the United States.

The Church of Scientology has reacted differently to the protesters' actions. One representative first claimed that the group's members "had obtained some erroneous information" regarding Scientology. One person described the group as "computer gurus." Later, the Church of Scientology began to describe Anonymous as *"cyberterrorists"* who were committing *"religious hate crimes"* against the organization.

Victim: Church of Scientology

2010 - Operation Payback

The hacking collective Anonymous launched Operation Payback, a series of cyberattacks in retaliation, against people who opposed Internet copyright theft. When numerous Bollywood studios hired Aiplex Software as a third party in 2010, they used it to perform distributed denial-of-service (DDoS) *assaults* against websites that did not react to requests for the removal of copyright-infringing content from their servers.

Operation Payback was launched in retaliation by Anonymous, who initially tried to bring down Aiplex Software using a DDoS attack (although they soon discovered that another individual had already done so a few hours before their planned coordinated attack).

The Motion Picture Association of America (MPAA), the International Federation of the Phonographic Industry (IFPI), the Recording Industry Association of America (RIAA), the British Phonographic Industry, and various law firms that prosecuted copyright infringement were among the targets of additional attacks against anti-copyright infringement organizations.

***Victim**:* Visa, Mastercard, Amazon, PayPal, Post Finance

2011 - Operation Tunisia

As is their custom, Anonymous launched a number of DDoS assaults against official websites. Additionally, Anonymous distributed a care package that included items like Tor and a greasemonkey script to prevent proxy interception by the government, as well as the documents needed to overthrow the current administration. Some people viewed the sharing of information as a component of Operation Leekspin. They also helped spread news of the protests both inside and outside the nation.

First, Anonymous released a YouTube video outlining its goals. DDoS assaults were started by Anonymous. As a result of the attacks, numerous official websites in Tunisia were quickly pulled offline. Through Tunisian blogger Slim Amamou, Anonymous provided anonymizing tools like Tor to the demonstrators. Large-scale professional strikes by Tunisia's professional class of attorneys and teachers were also taking place as the group launched its fight online, and this resulted with President Ben Ali departing on January 14, 2011.

A Tunisian blogger named Slim Amamou, also known by the handle "slim404," was one of the Anonymous participants in the #OpTunisia channel. He helped move software between Anonymous and the demonstrators. On January 6, 2011, Amamou was detained. In May, after being freed from prison and appointed secretary of state for sport and youth, he announced his resignation in opposition to the transitional government's web restrictions.

Victim: Tunisia Government

2011 - Fine Gael website attack

A group known for recent attacks on businesses involved in the WikiLeaks scandal has hacked into the website of Ireland's biggest opposition party. According to Fine Gael, the hackers known as

Anonymous compromised the personal information of up to 2,000 persons during the attack. The FBI is now participating in the inquiry, according to ElectionMall, an American online company that reported the cyberattack to US authorities.

In a statement, Fine Gael acknowledged that the Anonymous hacking collective, which has supported WikiLeaks and its founder Julian Assange against attempts by the US government to halt the disclosure of vital American diplomatic cables, was responsible for the infiltration of its website, Finegael.com. Attacks by Anonymous have been made on websites for businesses including: Allegations that Visa, Mastercard, and Amazon retaliated against WikiLeaks led to their suspension.

Following the online attack, Fine Gael informed Billy Hawkes' office, which is currently conducting an investigation. In connection with the issue, it also got in touch with the Garda computer crime unit. Fine Gael claimed in a statement that it had notified everyone who was impacted by email this morning. Since Fine Gael is most likely to be the dominant force in a new coalition after this year's Irish general election, which will be held in March, there doesn't seem to be a clear reason why Anonymous has attacked the party.

Victim: Fine Gael Irish political party

2015 - Cyberwar declaration against The Islamic State after Paris terrorist Attacks

The hacker collective Anonymous appears to have retaliated to the attacks in Paris by producing a video declaring war on the terrorist organization known as "Islamic State." A spokesperson wearing the group's recognizable Guy Fawkes mask declared in the unconfirmed YouTube video that the group of hackers will use their skills to wage "war" against the militant group.

Expect significant cyberattacks. It is declared *war*. Get ready," the French announcer adds. "Anonymous will look for you all across the world. You should be aware that we will track you down and won't let you escape. According to translated transcripts of the video, the speaker said, "We will conduct the largest operation ever against you’’. As part of its effort to create a caliphate, "Islamic State," or "IS," as it is also known, operates in some areas of Syria and Iraq. However, it has recently organized more attacks abroad, the most recent of which occurred on Friday and targeted a number of Parisian nightclubs, restaurants, and bars.

In Europe, a manhunt has started to find individuals who assisted the attackers, the majority of whom were wearing suicide belts. At the weekend, France replied by launching further airstrikes against IS strongholds in Syria. The latest video from Anonymous features a masked spokesman who declares in French that "the French people are stronger than you and will come out of this atrocity even stronger."

2020 - Black Lives Matter

The best-known hacktivist group on the world scene reappeared on the web issuing a warning following the murder of George Floyd, a 46-year-old African-American, while he was being arrested by police in Minneapolis, Minnesota, United States.

Floyd died of suffocation after spending 8 minutes and 46 seconds with Officer Chauvim's knee on his neck, the prosecutors' report states. Anonymous promised in a new video that it would show the criminal record of the Minneapolis police and expose the link between US President Donald Trump and the pedophile ring in the Epstein case, the 66-year-old billionaire accused of being involved in a network of sexual exploitation and trafficking of minors, who was found dead in his cell in the federal prison in Manhattan in New York.

"Unfortunately, in the vast majority of police killings, the only one left alive to tell the story is the officer who took the person's life," Anonymous says. With a questioning speech to the ruling class, the Anonymous video continues: “many people are now beginning to learn that you are not here to save us. If not, rather, you are here to oppress us and carry out the will of the criminal ruling class. In fact, you are the mechanism used by the elites to continue their global system of pressure. And he concludes: "Unfortunately, we do not trust your corrupt organization to carry out justice, so we will expose many of your crimes to the whole world."

The video was uploaded to Anonymous networks on May 28, but it went viral over the weekend on Twitter with the hashtag #Anonymous2020, and was later deleted from YouTube. According to various sources, the group would have been behind the interference to the radio used by the Minneapolis police to prevent agents from communicating with each other. A leak of emails and passwords from the Minneapolis police also circulated through the networks, although this information has not yet been confirmed.

However if any country has had linkings with the collective, therefore The United Nations could consider the possibility of applying penalties regarding the Budapest Convention of Cybercrimes made in 2004.

Case study 1: Black Little Book of Jeffrey Epstein

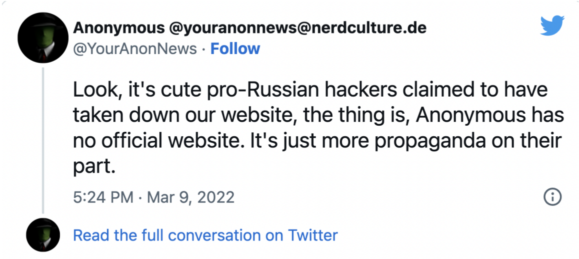
The June 2 of 2020, Anonymous after three years of inactivity, divulged what is known was supposed to be the star-studded address book of Jeffrey Epstein. Jeffrey Epstein was an American financial magnate, pedophile, and sexual predator, convicted of a network of trafficking minors in the elite world. Anonymous published a list of names that exposed multiple individuals who had contributed and collaborated with Jeffrey Epstein. It is relevant to consider that this event happened one week after the assassination of George Floyd under the police institution, which motivated anonymous to expose information that was hidden from the world by this institution, especially when there was a trial against him in 2008. Important world leaders such as Donald Trump and his family were involved in this book.

Case study 2: Tik Tok and the China Conspiracy

Since, the TikTok app started to be in the spotlight due to cybersecurity matters after in countries such as India, the app got banned, Anonymous took advantage of the situation and accused the Tik Tok platform of being an espionage tool controlled by the Chinese government. They posted a tweet saying: "essentially malware operated by the Chinese government running a massive spying operation." "Delete TikTok now". Therefore, they recalled the international community to erase this platform. This has outraged the concerns of censorship and political dissension.

Case study 3: Cyberwar declaration against Russia

In March 2022, there was a series of cyber attacks against the Russian government databases by anonymous hacktivists. They claimed responsibility for disabling prominent Russian Government, news, and corporate websites and leaking data from entities that were in charge of censoring the Russian media. Since then, Of 100 Russian databases that were analyzed, 92 had been compromised. There is no official report or declaration from part of Anonymous of the situation and their purposes like it has been explained in previous apparitions however, there have been multiple theories about this cyberwar declaration like it is the theory of punishment from part of the organization regarding Russia's invasion of Ukraine through mediatic sanctions. Other theories stated that countries may have interacted with the collective to organize an assault on the government's plans for this invasion.



Anonymous @youranonnews@nerdculture.de
@YourAnonNews · Follow

Look, it's cute pro-Russian hackers claimed to have taken down our website, the thing is, Anonymous has no official website. It's just more propaganda on their part.

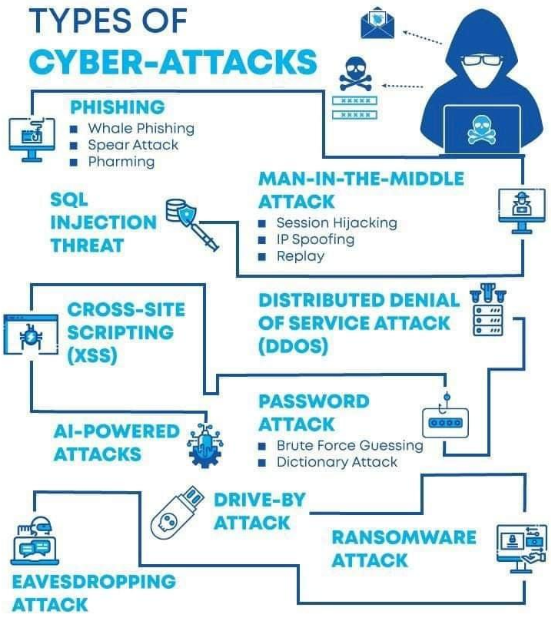
5:24 PM · Mar 9, 2022

Read the full conversation on Twitter

Retrieved-from::[*https://twitter.com/anonymous_co/status/1389497423366705155*](https://twitter.com/anonymous_co/status/1389497423366705155)

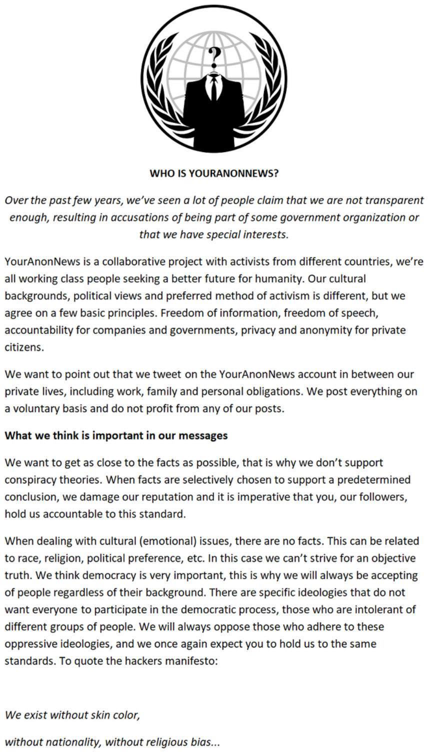
OBJECTIVES OF THE COMMITTEE

The Union of Cyber State Agents just take a decision on what is the international community committed to in order to capture and destruct the Anonymous organization. You should all take into account if the purposes of this organization are either beneficial or disruptive to the international media, and the information the global population receives. To capture them, the committee must research the past apparitions and insurgence along with their purposes and operations, being able to identify any connections or linkings with Anonymous from any individual, organization, or even country. Take into account all of the possible social responses and outcomes regarding past withdrawals and manifestations done in favor of Anonymous and its ideologies, and consider any sort of patterns or preferences towards the governments or institutions that had been victims. Consider what had been the targets for Anonymous to attack: Elite, public, or private organizations?; What type of governments?; Southern/northern country? Religious - by - consitution state?; Country with specific withdrawal/problem with the international community? Also research the types of different cyberattacks in order to find any strategy or prepare a counter-strike by using hack alternatives such as Malware, DDoS, Phishing, and BECs, among others, meanwhile the purposes are the one and only of counter-cyber-terrorism by Anonymous.



Retreieved from:[*https://www.complex.com/pop-culture/2011/08/the-10-craziest-anonymous-hacks/8*](https://www.complex.com/pop-culture/2011/08/the-10-craziest-anonymous-hacks/8)

Try to find any clues in order to identify possible future targets for Anonymous and hence, be ready for it and achieve its capture. Also, take into account that the nations must framework foreign policies and aims after the destruction of this collective, involving any sort of penalization or sanction considering article 19 of the Universal Declaration of Human Rights concerning the freedom of speech.



WHO IS YOURANONNEWS?

Over the past few years, we've seen a lot of people claim that we are not transparent enough, resulting in accusations of being part of some government organization or that we have special interests.

YourAnonNews is a collaborative project with activists from different countries, we're all working class people seeking a better future for humanity. Our cultural backgrounds, political views and preferred method of activism is different, but we agree on a few basic principles. Freedom of information, freedom of speech, accountability for companies and governments, privacy and anonymity for private citizens.

We want to point out that we tweet on the YourAnonNews account in between our private lives, including work, family and personal obligations. We post everything on a voluntary basis and do not profit from any of our posts.

What we think is important in our messages

We want to get as close to the facts as possible, that is why we don't support conspiracy theories. When facts are selectively chosen to support a predetermined conclusion, we damage our reputation and it is imperative that you, our followers, hold us accountable to this standard.

When dealing with cultural (emotional) issues, there are no facts. This can be related to race, religion, political preference, etc. In this case we can't strive for an objective truth. We think democracy is very important, this is why we will always be accepting of people regardless of their background. There are specific ideologies that do not want everyone to participate in the democratic process, those who are intolerant of different groups of people. We will always oppose those who adhere to these oppressive ideologies, and we once again expect you to hold us to the same standards. To quote the hackers manifesto:

We exist without skin color,

without nationality, without religious bias...

Retrieved-from: *https://mobile.twitter.com/anonindiapress*

GUIDING QUESTIONS

- Has your delegation/country's government or statal institution been a victim of Anonymous attacks?
- Has your delegation had a direct link with the Anonymous Collective?
- Has your government been a reason for protest for its population?
- Has your country signed the 2004 Budapest convention? Yes/No? Why?
- Has your country been responsible or has participated in any relevant cyber attack?

SOURCES

- *Anonymous Explained: Everything You Need To Know About The Hacktivist Group*. (2020, June 9). YouTube. https://www.youtube.com/watch?v=2cU2REZPVF4&feature=youtu.be
- Reuters. (2012, May 6). *Timeline Of Anonymous And Affiliates Cyber Attacks*. HuffPost. https://www.huffpost.com/entry/timeline-anonymous-cyber-attacks_n_1325459
- *The 10 Craziest Hacks Done By Anonymous*. (2020, May 31). Complex. https://www.complex.com/pop-culture/2011/08/the-10-craziest-anonymous-hacks/8
- (2022, March 16). *Anonymous declared a "cyber war" against*
- *Russia. Here are the results*. CNBC. https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

SUPPORT LINKS

- Support Link 1
- Support Link 2
- Support Link 3
- Support Lik 4