GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 12, Issue 5 May (2024)

VIRTUAL REPUBLIC

Tukhtasinov Alyorbek
Student of Nurafshon branch of Tashkent University of Information
Technologies (TUIT) named after Muhammad al-Khwarizmi
alyortuxtasinov2@gmail.com

Kuldoshev Otabek
Student of Nurafshon branch of Tashkent University of I
nformation Technologies (TUIT) named after Muhammad al-Khwarizmi
kuldoshevotabek87@gmail.com

ABSTRACT

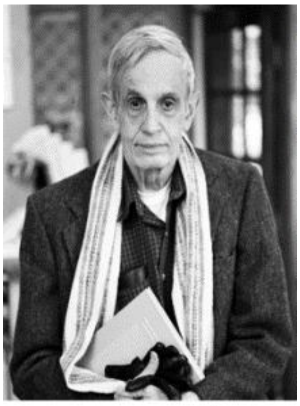
In the ever-evolving landscape of the Digital Age, a new concept is emerging - Virtual Republic. This article extends deep into the nation's paradigm run by hackers, exploring the consequences of their infiltration into our lives through a virtual republic. Revealing the activities, goals, and significance of this mysterious Virtual Republic is vital to understanding the complexities of our interconnected world.

Keywords. Virtual Republic, Virtual Nation, Hackers, Invasion, Cybersecurity, Digital Management, Online Activities.

1. Birth of a Virtual Republic

Virtual Republic is not limited to geographical boundaries, instead of that, it thrives on a complex network of internet. Run by groups of skilled hackers, this virtual nation challenges traditional notions of governance and sovereignty. As we study the essence of the Virtual Republic, we witness a digital landscape where the lines between **freedom**, **security** and **invasion** are blurred.

Today, when computer technology has become one of the most important aspects of our lives, this hidden threat is starting us in its path along with the work of entering our daily lives. There are now a lot of people around us who have their own PC. But among them are those who want to use the miracles of the century for outrageous purposes. This activity is referred to as hacking by the general public.


John Forbes Nash Jr.

The term "hacker" was originally used as an insult to those who solve mathematical issues in "circular ways." Its founder is the famous mathematician, **John Nash**.

At first, the hackers were involved in copyright programs with their own programs. Later, they were "committed" to changing the rules of the program for their own benefit. At the end of the day, conflicts and protests arose between the authors of the programs and users. Years later, the word "hacker" began to be interpreted completely differently. In the meantime, the term has become used against criminals who damage

computers, secretly enter them, install, and distribute viruses. Thus, today the hacking is aimed at reuniting the heads of outrageous targets, carrying out terrorist acts, stealing state secrets and large sums of money.
1) The 1st technological hack took place in 1972. By blowing the whistle, free calls were made. To do this, people used a whistle that came out of the Cap'nCrunch box. The frequency of whistle sound gave access to the telephone company's internal authentication system.
2) In the world, Ian Murphy is listed as the first hacker to be charged with a serious crime. He sneaked into the computer of AT&T in 1981 and changed his clock. This gave users the opportunity to call at night on a discounted tariff.
3) Kevin Mitnik was once the "most needed hacker" in the search. The servers it violates are DEC, IBM, PACIFIC BELL. Prosecutors believed Kevin Mitnick could also launch a nuclear weapon by blowing a whistle from a taxaphone.
4) Another hacker, Gerry McKinnon, has carried out the largest military hack in history. In 2001 and 2002, he secretly entered NASA, the US Army, navy, Military Air Force as well as Department of Defense servers through a network and carried out a theft that amounted to $ 800 thousand. He said he wanted to check if information about the NUJJs was kept secret.
5) The hacker sentenced to the longest prison term in US history is Albert Gonsales. He stole the numbers of credit and debit cards worth $ 200 million. The sentence is 20 years.
6) Us (hackers hacked) spam distributors have the largest number of computers. About 13.1% of spam distributed worldwide is distributed from the United States. India is 2nd with 7.3%. Brazil is ranked 3rd with 6.8%.
7) Virtual hacking schools in China earn $40 million a year. Students pay around 100 branches. The schools are believed to be involved in the attack on Google and US government sites.
8) Hackers worldwide are estimated to have embezzled intellectual property worth $1 trillion. Every year hacking causes $4 billion in damages to the US. And China will suffer $1 billion in damages.
(9) According to a 2009 survey, 43% of companies enriched their secrets to hackers.
(10) Each day, 1 in 3 companies faces hacking. 17% of these hacking attacks are successfully carried out. 81% of AT professionals consider their programs weak.
(11) Each year, a thousand hacking attacks on power plants. Hackers try to carry out terrorist acts and steal money. Millions of funds are stolen every year.
12) The Department of Defense will hire 250 hackers a year to protect against cyber threats in the US.
(13) In 2009, the Pentagon spent $6 billion on computer security. In the next 5 years, this indicator is expected to be between $ 15 and $ 20 billion per year.
14) The social networking site Facebook is on the list of sites where the most hacking attacks are launched. Hackers look for personal information such as phone numbers, passwords and letter correspondence.

2. Activities of the formation of a virtual nation

Within the Virtual Republic, hackers engage in multifaceted activities that affect our daily lives. Moral hackers, often considered defenders of a digital state, work tirelessly to identify vulnerabilities, strengthen cybersecurity, and strengthen our defenses. Instead, malicious hackers who work for a variety of motives exploit these vulnerabilities for personal gain, political agendas, or even specific disorder. Such hackers are usually divided into three types: Black Line, White Line and Grey Hat Hackers.

Black hat hacks, or simply "black hats", are the type of hacks popular media can usually think of. "Black-hat" hackers compromise the security of a computer for personal gain (such as stealing credit card numbers or collecting personal data to sell to identity thieves) or pure malice (such as creating a botnet and carrying out DDOS attacks to use this botnet) like a web T. Black hat fit a common stereotype where hackers are criminals who are illegally operating for personal gain and attack others. They are computer criminals.

White hat attackers' black hat is the opposite of hackers, who are experts who identify deficiencies in the security of "moral hackers," or computers, who use their capabilities for moral and legal purposes more than for bad and criminal purposes. For example, many White hat hackers work to verify the computer security of I organizations. The organization allows the white hat hacker to attempt to hack its systems. A white hat attacker uses his computer's knowledge of security systems to hack an organization's systems, like a black hacker. However, instead of stealing from the organization or vandalizing their systems, a white hat hacker helps the organization protect by reporting to the organization and reporting how it got to the organization. This is known as the "penetration investigation", and this is just one example of activity performed by White hat hackers. A white hat hacker who finds security flaws reveals it to the developer and they allow him to fix the product and improve his security. Very little in life belongs to black or white categories. In fact, there is often a gray area. The grey hat hack falls somewhere between the Black Line and the White Line. The gray hat does not work for its own personal gain or cause a revolt, but they can technically commit crimes and do things that are unethical. For example, a black hat hacker violates a computer system without permission and uses it to steal data or for their own personal gain. A white hat hacker system is breached by alerting the organization for security purposes and helps to eliminate the flaw. A gray hat hacker can corrupt a computer system without permission from the organization. In this case, although the hacker did not aim badly, it is illegal for them to violate the security system without permission.

3. Goals: Promoting the Motivations of the Virtual Republic

Understanding the goals and motivations of hackers within the Virtual Republic is patrimonial to understand its impact on our society. Some hackers aim to expose vulnerabilities in systems, causing improvements and contributing to the evolution of cybersecurity. Others are based on a spectrum of motivations, from financial gain to ideological beliefs, and use their skills to penetrate and break in. Turning off these motives provides insight into the dynamic relationships between technology, power, and individual ideas within a virtual nation.

4. **Importance of the Virtual Republic in** Modern Times

As our dependence on technology deepens, Virtual Republic plays a central role in shaping our present and future. The actions of hackers within this virtual nation have huge consequences affecting political landscapes, economic systems and social structures. Virtual Republic encourages us to rethink our approach to cybersecurity, stressing the need for proactive measures and ethical hacking practices. Data is a valuable commodity, and it highlights the fragility of our Virtual Republic digital presence in an era when information is a powerful weapon.

5. Balancing Principles: Ethical Hacking and Cybersecurity Measures

A delicate balancing should be triggered in the face of the challenges posed by the Virtual Republic. E skiing is considered a critical factor to strengthen our hacking defenses and stay one step ahead of malicious actors. Governments, businesses and individuals must cooperate to create robust cybersecurity measures that protect against invasions without compromising privacy and freedom. The Virtual Republic serves as a wake-up call, forcing us to embrace a proactive stance in securing our digital future.

CONCLUSIONS

The rise of the Virtual Republic forces us to confront the complex interaction between technology, governance and individual agency. A growing age of technology will force us to create a way of living in cooperation with this Virtual Republic. Virtual Republic is not only a product of the digital age, but also a reflection of the challenges and opportunities presented by our interconnected world. By understanding the motivations, activities, and goals within this virtual nation, we can chart a path to a future that is consistent with the values of Virtual Republican privacy, security and moral management. In this dynamic landscape, the Virtual Republic serves as the catalyst for change, which encourages us to adapt and strengthen our digital borders to the challenges ahead.

REFERENCES

1. Wikipediya — https://uz.wikipedia.org/wiki/John_Nash
2. Daryo.uz axborot internet nashri.
https://daryo.uz/2021/02/21/kiberxavfsizlik-2020-yilda-sodir-bolgan-eng-yirik-xakerlik hujumlari%2F?utm_source=%40daryo_lotin%2F
3. Alvarez Sanchez, D. (2018). From hacker culture to civic hacking. Valence
https://riunet.upv.es/handle/10251/111866

4. California Legislative Information. (2018). California Consumer Privacy Act (CCPA). Retrieved from https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
5. Elissa M. Redmiles. (2020). Toward the Science of Security and Privacy in Machine Learning. Google Schoolar.
6. https://movilforum.com/uz/axloqiy-xakerlik/
7. A. Akerlof, J. Shiller (2015). Phishing for Phools: The Economics of Manipulation and Deception. https://www.goodreads.com/author/show/1404728.George_A_Akerlof
8. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. https://theswissbay.ch/pdf/Books/Computer%20science/socialengineering_thescienceofhumanhacking_2ndedition.pdf