INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT,

ENGINEERING AND SOCIAL SCIENCES

ISSN: 2349-7793 Impact Factor: 6.876., Volume: 18 Issue: 02 in February 2024

GLOBAL THREATS IN THE VIRTUAL WORLD

Muhayyo Jalilova
Faculty of Social Economy of Andijan State University
Student of applied psychology

Annotation: the article is written on the topic of global cyber security. This article discusses the cyber threats of the virtual world and their impact on the physical world. The author presents how people can be addicted to the virtual world for their daily activities and the problems that occur on the network. The article also examines the dark side of the cyber world, and discusses what threats international security should deal with. At the end of the article, transnational security concerns and the required aspect of decision making are cited. Let's say the article presents globally important problems on the topic of cybersecurity and provides readers with the information they need to think about as a guide to combating global security deadlines

Keywords: Virtual world, global threat, cyber security, network,technology, computer.

In the last decade, people have become as dependent on the virtual world for their daily activities as they are on the physical world for human activities. Consider the consequences when a network goes down, mobile phone calls stop, or a virus disrupts the network. Often, daily routines are disrupted, feelings of despair rise, and work comes to a halt. There are clear advantages of information technologies that are essential for our lives, economy, and ultimately, national security.

Information technologies connect people in unique ways. Global optical fiber networks have facilitated unprecedented communication and contributed to India's emergence as the "back office" of the world, enabled companies to operate offshore, and allowed consumers access to diverse information across our planet. Nearly a quarter of the world's population uses the internet. This interconnectedness within and between societies has a significant impact on economic growth and development, especially in impoverished regions.

It also provides countries with the opportunity to overcome the challenges of geographic isolation or lack of access to developed major countries in North America, Europe, and Northern Asia.

In addition to the cultural impact of technology, there is also the dark side of the cyber world where hackers, phishing scammers, and transnational crime groups exploit technology. Criminals and spies can gain access to government and private computer networks through Trojan horses. Individuals and groups can disrupt governments and corporations by deploying viruses and denial-of-service attacks. And the use of spyware or government surveillance programs infringes on citizens' personal privacy rights. It is now possible to delete or steal personal, professional, and financial reports for malicious purposes, no longer a mere fantasy.

Thus, for many, the greatest threat to their personal security comes from cyberspace. Nevertheless, cyberspace is not only a personal issue but also a national security issue. Just yesterday, the Director of National Intelligence of the U.S. testified about this in the annual threat assessment:

ISSN 2349-7793 (online), Published by INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT, ENGINEERING AND SOCIAL SCIENCES.,
under Volume: 18 Issue: 02 in February-2024
https://www.gejournal.net/index.php/IJRCIESS

"We face a variety of access, technical complexity, and intent combinations from national states, terrorist networks, organized crime groups, individuals, and other cyber actors. Many of these actors are capable of targeting elements of U.S. information infrastructure to collect intelligence, steal or disrupt intellectual property."

While conflicts between China and Google have heightened interest in cybersecurity, personal hackers pose the greatest threat to information security. However, governments are now including cyber warfare in their planning and operations. A recent example is the cyber attack that occurred alongside Russia's invasion of Georgia in 2008. As Russian tanks and aircraft entered Georgian territory, cyber warriors attacked the Georgian Ministry of Defense. Although it had minimal impact, the attack was indicative; future conflicts will involve both physical and virtual dimensions. Governments and militaries, having adopted technology for efficiency and effectiveness, remain vulnerable to cyber threats. With much of society, government, and the economy shifting to online modes, people in developed countries can no longer be isolated from the effects of war.

However, virtual warfare does not necessarily accompany physical attacks typical of conventional warfare. Countries are increasingly employing cyber operations outside of armed conflict, indicating that cyber power is becoming a unique tool. On any given day, foreign governments sponsor breaches into other governments' networks, hackers steal financial data from banks, and foreign intelligence services engage in cyber espionage. Given the significance of information technology networks and the threats they face, awareness of cybersecurity is increasing.

Nevertheless, awareness has not yielded specific strategies for combating these threats. This is a component of the issue. The private sector primarily designs, builds, owns, and manages the internet, but there is growing reliance on the government to protect it. The Department of Defense is responsible for securing the “dot.mil” domain, while the Department of Homeland Security oversees the “dot.gov” domain. The “dot.com” domain is entrusted to the companies operating within it. However, as Director Blair's testimony clearly shows, neither governments nor the private sector alone can mitigate cyber threats.

The collaborative approach aligns with both the Obama administration's message and the changing nature of security. Modern security issues such as pandemics, piracy, or terrorism are transnational and require international cooperation. Unlike traditional threats, it does not matter whether the United States remains a superpower, NATO is the most advanced alliance in the world, or China and India are rising powers. Transnational threats impact citizen-level countries, and governments continue to struggle with how to address them.

Speed and secrecy lead to more successful attacks. Adversaries operate with unprecedented secrecy, and today’s attacks can achieve success in just a few minutes. They conceal themselves by using valid account credentials and legitimate tools, making it challenging for defenders to detect security breaches.

Individual-based attacks continue to rise. Identity threats surged in 2023. Adversaries like SCATTERED SPIDER, using generative artificial intelligence, are employing new methods for faster access, such as phishing, social engineering, and purchasing legitimate account credentials from

ISSN 2349-7793 (online), Published by INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT, ENGINEERING AND SOCIAL SCIENCES.,
under Volume: 18 Issue: 02 in February-2024
https://www.gejournal.net/index.php/IJRCIESS

access brokers. Tactics like SIM card swapping, bypassing two-factor authentication, and using stolen API keys for initial access are becoming more prevalent.

Adversaries Dominating the Cloud

Adversaries are leveraging the global adoption of cloud technology to turn the cloud into a primary battleground. Cloud-based adversaries, especially eCrime actors, use legitimate account credentials to gain access to victims' cloud environments and then employ lawful tools to carry out their attacks—making it difficult to distinguish between legitimate user activity and breaches.

Exploiting Interactions Opens Access to Multiple Victims

By targeting vendor-customer relationships, adversaries maximize their return on investment (ROI) by creating a single point of entry to target multiple organizations across verticals and regions. They use access to IT vendors and disrupt the software supply chain to distribute malicious tools through trusted applications.

Generative AI Poses New Adversary Threats

The misuse of generative AI by adversaries raises concerns about creating malicious software, tools, and resources for more sophisticated social engineering campaigns and stronger attacks. Trends from 2023 already show that AI has frequently been used for social engineering, and the power of AI provides adversaries with limitless opportunities to become more complex.

Recent research warns that the ICC Commercial Crime Services (CCS) sees an increasing risk of users transferring money and personal information online through online games. Commercial crime has long been a global phenomenon without borders. Now, internet security giant Symantec reports that virtual worlds like Second Life and World of Warcraft are being targeted by organized crime as money laundering tools.

Symantec's recently released Internet Security Threats Report forecasts that as the use and popularity of virtual environments expand, they will increasingly face threats from organized crime. Symantec predicts a range of security issues over the next six to 24 months, highlighting money laundering and identity theft among potential problems.

Max Vetter of ICC Commercial Crime Services (CCS) stated: "Symantec's latest findings raise significant concerns about the potential misuse of new technologies by major criminal enterprises. Users of some online games need to make every effort to protect themselves from theft and fraud."

The nature and operation of virtual worlds like Second Life make them attractive to those seeking to transfer funds quickly and anonymously. Massively Multiplayer Online Games (MMOGs) like Second Life and World of Warcraft allow players to conduct transactions with real money in virtual worlds. Players can use credit cards or other payment methods to purchase virtual credits, which can then be exchanged with other players in different countries and easily converted into local currency. These operations have effectively turned into an international currency system with sophisticated exchanges designed for virtual currency trading in various MMOGs.

ISSN 2349-7793 (online), Published by INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT, ENGINEERING AND SOCIAL SCIENCES.,
under Volume: 18 Issue: 02 in February-2024
https://www.gejournal.net/index.php/IJRCIESS

Mr. Vetter added: “Although the scale of criminal activity in this area is currently not very significant, this is precisely why we want to focus on it. It is crucial to identify and monitor such unregulated money exchanges before criminal elements enter.”

Symantec's report details: “A criminal organization may open several thousand MMOG accounts. Each of these can be used to trade in-game assets with other players or purchase and sell virtual goods, with funds eventually withdrawn from the accounts. Since thousands of accounts can execute millions of transactions with each transaction having a small profit or loss, it becomes difficult to trace the actual source of funds when they are withdrawn. These transactions can occur worldwide, often accompanying international bank transfers, without oversight. In fact, in February 2007, China’s central bank and finance ministries urged companies to halt trading in QQ coins and virtual currencies, possibly to restrict unregulated currency exchange.”

Acting on the Latest Threats

In the second half of the year, we have observed significant activity among APT groups, more targeted payment software attacks, new botnets and strains of malware, and increased exploitation of IoT devices. We have also witnessed a rise in complex attacks targeting large enterprises and critical networks.

REFERENCES

1. Madumarov, T., & Ogli, G. O. R. (2023). O’ZBEKISTON RESPUBLIKASIDA KORRUPSIYAGA QARSHI KURASHISH (TA’LIM TIZIMI MISOLIDA). Ta’lim fidoyilari, 2(1), 194-197.
2. Ибрахимов, Б. (2023). ПОНЯТИЕ И ОСОБЕННОСТИ “ГЛУБОКИХ ФЕЙКОВ”. Namangan davlat universiteti Ilmiy axborotnomasi, (6), 201-206.
3. Nasriddinovich, A. A. (2021). Civil society and the transformation of islamic values. ACADEMICIA: An International Multidisciplinary Research Journal, 11(3), 709-714.
4. ДУМАРОВ, М. Х. ЁШЛАР ИЖТИМОИЙ РЕАЛЛИК ИДРОКИНИНГ ЎЗИГА ХОС ЖИҲАТЛАРИНИ ЭМПИРИК ЎРГАНИЛИШИ. PSIXOLOGIYA Учредители: Бухарский государственный университет, (1), 149-153.
5. https://www.atlanticcouncil.org/blogs/new-atlanticist/virtual-threats-in-the-real-world-the-challenge-of-cyberspace
6. https://www.crowdstrike.com/global-threat-report/
7. https://iccwbo.org/news-publications/news/virtual-money-laundering-threat-identified/
8. https://www.fortinet.com/resources/analyst-reports/threat-report-2h-2023

ISSN 2349-7793 (online), Published by INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT, ENGINEERING AND SOCIAL SCIENCES.,
under Volume: 18 Issue: 02 in February-2024
https://www.gejournal.net/index.php/IJRCIESS