**ПРАВО ЗАРУБЕЖНЫХ СТРАН:
ПРОБЛЕМЫ ТЕОРИИ И ПРАКТИКИ**

**LAW OF FOREIGN COUNTRIES:
PROBLEMS OF THEORY AND PRACTICE**

УДК 327

DOI 10.33184/pravgos-2020.4.17

CYBER WARFARE – A POTENTIAL GLOBAL THREAT

BAJAJ Amay

Advocate, Madhya Pradesh High Court, India; Certified in IPR (WIPO, United Nations, Geneva); Advance Diploma in Cyber Laws, Pune, India

E-mail: adv.amaybajaj@gmail.com

This research article focuses on the concept of cyber warfare becoming a potential global threat. **Purpose:** to cover the basics of hacking, ethical hacking, cyber warfare, types of threat, cyber-attacks and cyber counter-intelligence. The article explains how hacking is done and what are the requisites for ethical hacking. In 2020, what all cyber threats, we are subjected to and how to counter it. **Methods:** the research is based on the methods of analysis, synthesis and description. **Results:** the article describes how cyber warfare could be a medium of war in future and how different nations are using technology to gain power as well as defend themselves from multi-potential threats.

Keywords: cyber-attack; cyber warfare; hacking; threat; cyber counter-intelligence.

Hacking. Definition. The New Hacker's Dictionary, a resource used to elucidate upon the art of computer hacking has defined the practice through an assortment of definitions:

- a hacker may be defined as any person who enjoys exploring the intricacies of programmable systems and how to stretch their capabilities. This definition is held in contrast to a generic computer user, who prefers to access a computer's minimal functions;
- one who programs or who enjoys programming, as opposed to those individuals who simply theorize about programming;
- an individual who possesses exceptional skill regarding computer programming;

– a malicious meddler who attempts to discover and subsequently tamper with sensitive information through poking around computer-based technologies. These individuals are commonly referred to as «network hackers» or «password hackers».

Regardless of the definition, there are unwritten rules or principles that a hacker will ultimately live by. The belief that information sharing is a powerful exercise and that is the ethical duty of hackers to share their expertise through the creation of free software and through facilitating access to information and to computing resources is a fundamental code for which the majority of hackers follow. In addition, computer hacking as a practice revolves around the belief that system cracking as a hobby or for fun is ethically okay so long as the hacker commits no vandalism, theft or a breach of confidentiality.

Description. Computer Hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. An attempt to exploit a computer system or a private network inside a computer.

Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose. Those individuals who engage in computer hacking activities are typically referred to as «hackers».

To better describe hacking, «one need to first understand hackers. One can easily assume them to be intelligent and highly skilled in computers. In fact, breaking a security system requires more intelligence and expertise than actually creating one» [1].

There are no hard and fast rules whereby we can categorize hackers into neat compartments. However, «in general computer parlance, we call them white hats, black hats and grey hats. White hat professionals hack to check their own security systems to make it more hack-proof. In most cases, they are part of the same organization» [1].

Black hats hackers hack to take control over the system for personal gains.

Grey hat hackers «comprise curious people who have just about enough computer language skills to enable them to hack a system to locate potential loopholes in the network security system» [1]. The impact of computer hacking will vary from a simple invasive procedure to an illegal extraction of confidential or personal information.

Issues of Computer Hacking. Computer hacking possesses a mixed perception. Due to our reliance on computer technologies and the critical information shared on network, the art of computer hacking has been skeptically viewed. That being said, there is also a «Robin Hood» mentality attached to the practice where free programs or facilitated measures have been awarded to the average

computer user. The primary issue attached to computer hacking stems from an individual's ability to access crucial to personal information that is found on a computer network. The ability to retrieve and subsequently tamper with such information will give way to the potential to commit heinous criminal acts.

Ethical hacking. Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the action and intent of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing or red teaming. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. By conducting penetration tests, an ethical hacker looks to answer the following four basic questions:

- what information/locations/systems can an attacker gain access?
- what can an attacker see on the target?
- what can an attacker do with available information?
- does anyone at the target system notice the attempts?

An ethical hacker operates with the knowledge and permission of the organization for which they are trying to defend. In some cases, the organization will neglect to inform their information security team of the activities that will be carried out by an ethical hacker in an attempt to test the effectiveness of the information security team. This is referred to as a double-blind environment. In order to operate effectively and legally, an ethical hacker must be informed of the assets that should be protected, potential threat sources, and the extent to which the organization will support an ethical hacker's efforts.

Cyber warfare. Cyberwarfare involves the use and targeting of computers and networks in warfare. It involves both offensive and defensive operations pertaining to the threat of cyberattacks, espionage and sabotage. There has been controversy over whether such operations can duly be called «war». Nevertheless, nations have been developing their capabilities and engaged in cyberwarfare either as an offender, victim or both. Cyberwarfare has been defined as «actions by a nation state to penetrate another nation's computers or network for the purposes of causing damage or disruption» [2], but other definitions also include non-state factors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists and transnational criminal organizations. Some governments have made it an integral part of their overall military strategy, with some having invested heavily in cyber warfare capability. Cyber warfare is essentially a formalized version of penetration testing in which a government entity has established it as a warfighting capability. This capability uses the same set of penetration testing methodologies but applies them, in the case of United States doctrine, in a strategic way to:

- prevent cyberattacks against critical infrastructure;

- reduce national vulnerability to cyberattacks;
- minimize damage and recovery time from cyberattacks.

Offensive operations are also part of these national level strategies for officially declared ward as well as undeclared secretive operations.

Cyber attacks. Indiscriminate attacks. These attacks are wide-ranging, global and do not seem to discriminate among governments and companies. Examples:

- operation Shady RAT;
- world of Hell

Destructive attacks. These attacks relate to inflicting damage on specific organizations. Examples:

- Great Hacker War and purported «gang war» in cyberspace;
- Lulz Raft, hacker group known for a low impact attack in Canada;
- Operation Ababil conducted against American financial institutions;
- Vulcanbot.

Cyberwarfare. These are politically motivated destructive attacks aimed at sabotage and espionage. Examples:

- 2010 cyberattacks on Burma, related to the 2010 Burmese general election;
- 2010 Japan – South Korea cyber warfare;
- 2013 Singapore cyberattacks, attack by Anonymous in response to web censorship regulations in the country, especially on news outlets;
- July 2009 cyberattacks, against South Korea and United States.

Government Espionage. These attacks relate to stealing information from/about government organizations. Examples:

- 2008 cyberattack on United States, cyber espionage targeting U.S. military computers;
- Cyber attack during the Paris G20 Summit, targeting G-20 related documents including financial information;
- GhostNet;
- Moonlight Maze;
- Operation Newscaster, cyber espionage covert operation allegedly conducted by Iran;
- Operation Cleaver, cyber warfare covert operation allegedly conducted by Iran;
- Shadow Network, attacks on India by China;
- Titan Rain, targeting defense contractors in U.S.;
- Office of Personnel Management data breach - Dec 2014 breach of data on U.S. govt, employees;
- A 6 month long cyber attack on the German parliament for which the Sofacy group is suspected, took place in December 2014.

Corporate Espionage. These attacks related to stealing data from corporations related to proprietary methods or emerging products/services. Examples:

- Opeartion Aurora;
- Operation Socialist, U.K. obtaining information from Belgian telecom company on call information;
- Sony Pictures Entertainment hack.

Stolen e-mail addresses and Login credentials. These attacks related to stealing login information for specific web resources. Examples:

- 2011 Playstation Network outage, network disruption;
- Gawker – 2010, rooted the servers;
- IEEE – September 2012, 100 000 members affected;
- Living Social – 2014, 50 million users affected;
- Adobe – 2013, source code theft, 150 million users affected;
- Rock You – 2009, data breach, 32 million user accounts;
- Yahoo – 2012, 2013, 2014, 453 000 user accounts compromised.

Stolen credit card and financial data:

- 2016 Indian Banks data breach. It was estimated that 3.2 million debit cars were compromised. Major Indian banks – SBI, HDFC, ICICI, YES BANK & AXIS BANK were amongst the worst hit;
- 2014 JP Morgan Chase data breach by Russian Hackers;
- Master Card 2005 – 40 million cards hacked;
- VISA&Master Car 2012 – 10 million credit cards hacked;
- StarDust 2013 – 20 000 cards hitting U.S. merchants;
- Target 2013 – 110 million customers affected;
- Home Depot – Sep 2014, 56 million payment cards affected.

Stolen medical – related data. By May 2017, three healthcare payer organizations had been attacked in the U.S.: Anthem, Premera Blue Cross and Care First. The three attacks together netted information on more than 91 million people.

Hacktivism. Politically motivated hacktivism includes the subversive use of computers and computer networks to promote an agenda and can potentially extend to attacks, theft and virtual sabotage that could be seen as cyber warfare or mistaken for it.

Cyber counter – intelligence. Cyber counter – «intelligence are measures to identify, penetrate or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions» [3].

On April 7, 2009, The «Pentagon announced they spent more than \$100 million responding to and repairing damage from cyberattacks and other computer

network problems. On April 1, 2009, U.S. lawmakers pushed for the appointment of a White House cyber security «czar» to dramatically escalate U.S. defenses against cyberattacks, crafting proposals that would empower the government to set and enforce security standard for private industry for the first time» [3]. On February 9, 2009, «The White House announced that it will conduct a review of the nation's cyber security to ensure that the Federal Government of the United States cyber security initiatives are appropriately integrated, resourced and coordinated with the United States Congress and the private sector» [3].

Conclusion. Cyber warfare is a latest trend of war tactics in which countries may involve themselves in war and inflicting harm to the people and resources without actually being involved physically. Developed nations and the United Nations shall look after this global threat and form policies to maintain peace and prosperity. As «Peace hath her victories no less renowned than war».

References

1. Definition of «Hacking» – The Economic Times. Available at: <http://economictimes.indiatimes.com/definition/Hacking?prtpage=1>.
2. Polonskaya O.Y., Kushnareva T.V. The concept of «Cyberwarfare»: actualization in publicistic discourse. *Sovremennoe pedagogicheskoe obrazovanie = Modern teacher education*, 2020, no. 4, pp. 219–221.
3. Andress J. Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. Available at: <https://docviewer.yandex.ru/view/28245995>.

Received: 29.10.2020

КИБЕРВОЙНА – ПОТЕНЦИАЛЬНАЯ ГЛОБАЛЬНАЯ УГРОЗА

ЭМЕЙ Баджадж

Адвокат Высокого суда Мадхья-Прадеша, Индия; диплом специалиста в области защиты прав интеллектуальной собственности (ВОИС, ООН, Женева); диплом специалиста в области киберзаконодательства, Пуна, Индия
E-mail: adv.amaybajaj@gmail.com

В статье основное внимание уделяется концепции кибервойны, которая становится потенциальной глобальной угрозой. **Цель:** рассмотреть ос-

новые характеристики взлома, этического взлома, кибервойны, типов угроз, кибератак и киберконтрразведки. Дается объяснение тому, как осуществляется взлом и что необходимо для этического взлома. Рассматриваются актуальные киберугрозы, появившиеся в 2020 г., и возможные средства противостоять им. **Методы:** в основе исследования лежат методы анализа, синтеза и описания. **Результаты:** раскрывается, как кибервойна может стать средством ведения войны в будущем и как разные страны используют технологии для получения власти, а также для защиты от множественных потенциальных угроз.

Ключевые слова: кибератака; кибервойна; взлом; угроза; киберконтрразведка.

Библиографический список

1. Definition of «Hacking» – The Economic Times URL: <http://economictimes.indiatimes.com/definition/Hacking?prtpage=1>.
2. Polonskaya O.Y., Kushnareva T.V. The concept of «Cyberwarfare»: actualization in publicistic discourse // Современное педагогическое образование. 2020. № 4. С. 219–221.
3. Andress J. Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. URL: <https://docviewer.yandex.ru/view/28245995>.

Дата поступления: 29.10.2020