# STUDY OF THE IMBALANCE AND DISPROPORTIONS IN THE OPPOSITION OF CYBER DEFENSE AGAINST HACKERS

Assoc. Prof. PhD Dimitrov W.
Faculty of Information Technologies – University of Librarian Studies and Information Technologies, Bulgaria
v.dimitrov@unibit.bg

***Abstract:*** *Study outlines the contours and the magnitude of the asymmetry in the opposition of cyber defense against hackers. Propose a model that reflects the dynamics of the opposition on both sides and the impact of the listed disproportions. It consist a functional analysis of the differences between organizational and technical approaches applied from both sides. Contains research into why even the most highly protected systems suffer from successful hacking attacks. The analysis sheds light on the magnitude of pressure exerted by malicious actors on cyber security for organizations and the disproportionate response from experts who protect information systems and networks.*

.

**Keywords**: CYBER, SECURITY, DEFENCE, HAKER, VULNERABILITY, INFORMATION, SYSTEM, OPPOSITION

## *1. Introduction*

Increasing the reach of the cyber physical world is reducing its ability to protect against malicious intrusion. The scope of modern cyber incidents clearly shows that this process is deepening. This article is focused in the breaking of the balance between the forces of information systems defenders and attackers. The study considers the characteristics of the balance of forces on both sides. Outlines the contours and the magnitude of the asymmetry in this disproportion. Proposes a model that reflects the dynamics of the opposition on both sides and the impact of the listed disproportions.

## *2. Methodology of study*

A wide range of approaches are applied creating this research: continuous personal observations on the work of cybersecurity teams serving complex information systems and networks of large private and public organizations, reviews into studies of well-established cyber security companies, regulatory requirements, analysis of research from scientific publications.

Let the surface tension on the vulnerabilities space be characterized by the organizational, expert and technological capabilities of the attackers and defenders. The potential for defense and attack is formed by the organizational capabilities - O, the state of expertise - E, and the technological equipment - T.

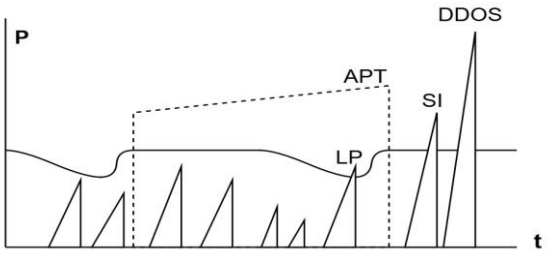


***Fig. 1*** *The dynamics of the vulnerability surface stress*

This are two vectors (O, E, T) opposite in direction. The proportion of the size of these vectors is the stress on the surface of vulnerabilities. On the graph, this is the parameter P (see Fig. 1). Table 1 contains brief explanations for the individual parameters. It lists properties of the disproportions.

The downturns in the chart reflect a weakening of the security. The fig. 1 shows that low profile (LP) attacks are facilitated at certain times when the defense weakens. Such moments are related to team fatigue, organizational changes - mergers or acquisitions, changes to the security team or the emergence of new sophisticated tools in the hands of attackers. Usual types of attacks SI and DDoS are successful in general. APT are attacks carried out with sophisticated assault tools produced with the support of state institutions.

.

Security managers work in a pressurized environment which seems to create new varieties of stress on a regular basis. The overall threat level continues to grow. Beyond that, however, the "surface area" of risk exposure expands over time. In tandem, the number of security alerts increases creating a situation where staffers and their incident response capacity can become overwhelmed [1].

***Table 1:*** *Parameters used on Fig. 1.*

| Parameter | Explanation | Note |
|---|---|---|
| P | (O,E,T) Stress of the Surface of vulnerabilities | Potential of Synergy between organizational, expertize and technological abilities |
| t | time | In general SLA for security services |
| APT | Advanced Persistent Threats | High profile attack with stealth continuous presence of adversaries |
| LP | Low Profile Attack | It's more possible attack, Facilitated in certain circumstances |
| SI | Security Incident | Regular security incident within regular state of protection |
| DDOS | Distributed Denial of Service | High Profile Attacks, incl. DRDOS and others |

The rest of the article contains basic counterpoints that confirm the model described.

**The attack goes quickly, the consequences are eliminated for years.** After a break is detected, closure measures are usually taken as soon as possible, if possible. An investigation into the incident then begins, and regulations under company laws and policies require that the affected counterparties, consumers and customers are notified and often compensated. Often these processes go on for years.

**Defenders are forced to take care of accidental or deliberate threats from insiders**, while attackers have no similar commitment. People create conditions for further expansion into the threat surface.

**The expertise of online attackers is deeply focused in a particular problem area**, and defenders are required to respond to a variety of attacks across a wide range of problem areas [2]. High profile attacks by different attacker groups are dispersed across a wide range of areas of knowledge for information technology and networks.

**Complex hacking tools are available to ordinary, poorly trained users.** Complex attacks are already under the power of

everyone [3]. Refined attacks are being carried out today by inexperienced users [4]. Attacks that exploit known vulnerabilities using freely available hacking tools, with little expertise required to be successful [5].

**Unprepared users can compromise strong protection.** The hacker has promised to release information on 20,000 FBI agents and 9,000 homeland security officials following an attack by a social engineering method against the US Department of Justice. Information has expired, which includes names, email addresses, phone numbers and job descriptions for thousands of employees. The hacker claims that the information received became available after the DOJ's email account was first compromised. The specialist then uses a surprisingly simple method to attack with social engineering and gains access to the DOJ's internal network. The hacker claims that he achieved all this by a phone call to the Ministry of Justice. Introduces yourself to a new employee who cannot access the DOJ web portal. "So I called and told them I was new and didn't understand how to get into the portal," says the hacker with a nickname motherboard. "They asked me if I had a token to go in, and I said I didn't have a symbolic code. They answered me: just use one of ours." Due to its limited time, it only retrieves 200 gigabytes of data that contains information about FBI and DHS employees, but claims that the database also includes military emails and credit card numbers [6], [7].

**The news of the threats is developing intensively, and counter-measures are slow, with a constantly lagging pace.** "The cyber security landscape is characterized by rapidly evolving threats and vulnerabilities against the slower implementation and deployment of defense measures."[8] Mitigating and responding to cyber threats are hampered by inadequate government-industry information exchange processes, lack of security, specific technological and human resources, and the challenges posed by multiple jurisdictions in the aftermath of threats. [9]

**Predictabily.** If the organization is compliant with PCI-DSS v 3.0 it is a clue for the adversaries not to toward that measures. The isolated security mechanisms, however effective, are inherently insecure as they become predictable. Their predictability makes it possible for people to 'hack' the security. The layered security, on the other hand, is like a complex threat response. It introduces unpredictability that makes it much harder to subvert the system [10].

**The attackers can repeat the attacks to infinity, but the defenders have the ultimate ability to handle a limited number of security incidents at the same time.** This inevitably causes the victims to collapse.

**A false sense of security [11].** Managers do not have a real appreciation for the security of their ICT (Information and Communication technologies) assets, although many of the risks to the businesses of the companies they work for depend on it [12], [13], [14]. For example, Australian managers do not have a real assessment of security issues. When IBM polls 5600 C-level executives, they find that 336 of them are "ostriches." That is, they have buried their heads in the sand, claiming that there is no room for breakthroughs in the security of computers that can significantly affect their organization. In fact, most respondents were more realistic about the threats - 94% thought there was a likelihood of a major cyber security incident in the next two years.

However, the latest IBM study found a significant group still holding their heads in the sand, although cybercrime is expected to cost global businesses in Australia up to AUS 800bn in one year, according to the Center for Strategic International Studies.

And a recent IBM report, based on interviews with 700 international C-level executives, including a significant number from Australia, found that even among senior government officials, there are those who do not understand the problem, there is confusion about which groups represent the biggest security threats and how to combat them effectively.

The report [15], [16] emerge indicating that even well-funded financial institutions aren't faring much better when it comes to their internal networks.

Complicating systems leads to an increase in attack surface. This is confirmed most of all over time. It happened with the spread of virtualization. All virtualized platforms remain intrinsic to the threats and a range of vulnerabilities that develop over time. At the same time, new vulnerabilities have emerged that naturally speak to extending the surface to threats. Examples to support those claims are the ability to copy usernames and passwords when transferring images of virtual machines through communication channels for backup or continuity of work, the emergence of new types of malware, called virtual machine avoidance (VM escape), in which the malware learns that it is in a virtual machine and, through its built-in functionality, is transferred to the host where the hypervisor operates [17]. A similar effect of expanding attack surface appears after the massive entry of containers, artificial intelligence, DLT (Distributed Ledger Technology), SDN (Software Defined Networks) [18], [19], [20], [21], [22].

**Cyber security experts gap.** At the beginning of the lifecycle of all products with these technologies, developers with expertise in design security are required. The problem with the lack of personnel affects the entire product life cycle information systems and networks, which they require support and updates.

At the same time the opponents are demonstrating increased professionalism and commercialization of the malicious activities and threats that are increasingly being adapted to specific regions. This is very motivating for malicious actors. Company employees are motivated mainly by their regular salary and possibly bonuses.

**Commercialization of leads to increase in the number of multi-level attacks [23].** Attacks that end with ransomware usually have a preliminary stage, during which all data that can be sold on the black market is leaked.

**The constant detection of new vulnerabilities brings outdated versions to zero-day forever.** Zero-day vulnerabilities are rarely the entry point to an attack. Much easier and more effective is the approach using old bugs. Examples are operating systems such as Windows XP, Windows 7, browsers such as Internet Explorer v. 10 or earlier, as well as any software artifacts that have not been provided with security updates for a long time. Some go as far back as 2012 [24], 2007 [25] and are extremely easy to find. The newcomers in cybersecurity don't know about them.

**Security requires continuous monitoring as opposed to attacks that are predominantly discrete and fast at their essential stage.** At the same time, if there are gaps in its implementation, continuous monitoring can be carried out simultaneously with presence of long-term housed and active agents with the properties of APT. The condition for continuity is duty of the team that implements security monitoring. They must fulfill the security requirements 24/7. This mode involves dissipation, a decrease in concentration over time, a blunting of risk sensitivities. Let's see the situation of a hacker invasion of such a SI, which is a mode of continuous security support. From the point of view of the invaders, even with long preparation, the attack is carried out with concentration of effort and attention. The focus is one weakness, say a 0-day vulnerability or social engineering, accompanied by surprise or no notice at all. The invaders take their data or other value resource, possibly hide their tracks and disappear. Security requires constant monitoring. Information security experts agree: One of the biggest challenges for protecting the corporate network is identifying threats and monitoring for unexpected changes before they can be misused. This requires continuous monitoring of the network and immediate and active resolution of potential problems.

Benefits of continuous monitoring include: complete security coverage of all networks and devices; accurate, prioritized results; reduced cost of guaranteeing security and compliance with standards; the ability to grow to millions of assets.

The question remains of the pertinent business objectives of building a perimeter to protect and evaluate risk [26].

**The implementation of multiple security measures does not guarantee complete security.** Along with the paradox of the contradiction between the continuity of security monitoring, we see a complementary a paradox in the range of the surface with vulnerabilities, which is protected against the focus of the invaders into one single vulnerability. This paradox is exacerbated by the regular situation that defenders deal with many known vulnerabilities, and the invaders with a single, but unknown to anyone but them. The following contradiction can be characterized by the phrase "alone against all". Leveling in preparation and even lacking, against high professionalism and refined tools.

Some of the certification programs for security professionals are produced by experts who do not have advanced training in software-related technologies, have no practical experience writing software code, testing, deployment processes, and maintenance issues, are not thoroughly familiar with computer architectures, let alone topics such as emission security. This allows them to perform many valuable and useful activities, but for the intricacies of software code security, architectures of major software systems and integration projects, thorough mature knowledge is needed, combined theoretically and practically, as hackers do not waste their time and apply them. They would not be able to implement an APT tool without thorough theoretical and practical training. Only one exploit kit that organizes a pipeline of exploits after a single victim used in a single campaign infects 1.25 million casualties in six weeks [27], [28]. According [29] companys' File Anti-Virus logged 187,597,494 unique malicious and potentially unwanted objects.

**The advantage of unfair attacks**. Defenders must be able to stop any type of attack to prevent their systems from being compromised while attackers perform their actions once to achieve their goals and win. The invaders know this and it is the reason that they try different methods of attack against the ICT systems of many organizations, in the expectation that one of the attacks will ultimately be successful. Even rigorous targeted attacks are repeatedly tried against the same system to ensure that any of the refined phishing emails will eventually reach the target.

**Attacks are AUTOMATED.** Dark Side opponents are capable of launching a large number of new attacks against a wide range of targets because they are armed with an arsenal of easy-to-use and effective tools. Hacker toolkits such as Magnitude and RIG allow malicious software to attack in a manner similar to a factory assembly line. For example, they search for online systems with common vulnerabilities and then send millions of malicious phishing messages to gain valuable sensitive data [30].

Magnitude is organized in two functionalities. The first contains a set of exploits and checks a potential victim with each of them. The set is dynamic because over time, some of the exploits become meaningless due to the closure of various vulnerabilities, often zero-day ones. The second contains various types of malware loads that can be installed after the exploit overcomes victim protection. The list of loads that this kit installed in 2014 includes ZeuS, Andromeda, Dorkbot/Ngrbot, Advertisement clicking malware, Tinba/Zusy, Necurs.

Other famous exploit kits in recent years are Angler, Nuclear and Neutrino. In the last quarter of 2015, 3.5 million attacks were initiated with this type of tool, according to [31].

**Attackers make money.** In the world of cybercrime, it's all business. Nowadays, such attacks feed fast-growing, illegal business empires. They make money from stolen credit cards, bank accounts, medical records and even corporate intellectual property. The attackers are ready to invest in complete exploits, new malware options and other attack tools because they know that the profits will be huge and their investment returns many times over.

**The bad guys refine faster than the good guys.** The attack on the Ukraine power grid in 2015 was low in sophistication but high in organization. Bad guys are intensively sharing information on the Dark Web, which gives them several benefits, such as the rapid development of intrusion attack tools, exploits, bot nets, renouncers, etc.; the continued depreciation of these instruments; opportunities to buy compromised data, including personal and interesting user accounts, along with passwords ...[32]. For $15, software tools can now be purchased and used by users without special training. A few years ago, the same operations required a high and rare qualification. That is, the bad guys are increasingly armed with tools, competencies, and have a data market that allows them to quickly become even worse.

Unlike the good ones, they sometimes have to refrain from sharing information because of the risk of compromising their entire business. They believe that if they illuminate and share their vicissitudes with others, they will encourage new and new users to join the bad side and simply repeat the attacks by the mechanisms described.

The second in the history of the attack (after Stuxnet), in which physical industrial systems are manipulated, is at an unnamed steel plant in Germany, described in the report, but Madnik notes that the factories negate the event, even though the damage to the steel smelter was serious [33]. Attempts to share information between good ones are fragmented so far. Major oil companies, for example, share information about cyber-attacks, but only with one another and do not pass it on to smaller ones.

**Hackers live in the future, and organizations carry the cyber-karma of the past.** Recently, a fact observed in [34] has indeed been observed. Governments are often constrained by the legacy of IT infrastructure, which can hamper efforts to strengthen their overall cyber security. Approximately three quarters of all government IT spending will support existing systems (computer systems and technologies that are often outdated or in need of replacement). Although cyber security is a high priority for the government, the budget is still shrinking. Such constraints reduce the potential of agencies as they seek to do more with less [34] .

**Massive cyberspace pollution without remediation mechanisms.** When an oil ship spills into the ocean, legal and public opinion emerge on the scene in order to punish the guilty and end such practices. When companies flood cyberspace with devices and applications that pose risks to business and privacy, the consequences so far are to release patches, new versions, and records in vulnerabilities registers. Hundreds of thousands of xDSL devices with built-in passwords by default, millions of instances with Android tare, millions of Heartbleed operating environments to date. Not only is the cleanliness of the seas important for the normal life of the planet... In conclusion, it is worth proposing a new term 'cyber space pollution'. It denotes huge amount of hardware and software, as well as digital systems of any caliber with security weaknesses. This will increase the capabilities of defenders of information systems and networks.

## *Conclusions*

A high level of organization is required to eliminate the consequences of a security incident. Listed disparities determining the successes of the invaders, who drain data, shut down services and in any way compromise the businesses of the companies. The systematic list contains an analysis of the inconsistencies of the protection of information systems and networks related to the attackers' methods. The list is useful to anyone who is into the issue or designing and maintaining IT security systems.

## *Acknowledgement*

This work has been developed following the activities of project "Research and analysis of the potential of new technologies for decentralized asset management", NIP 2019-13.

## *Literature*


[1] SWIMLINE, *Automating Incident Response*, 2018. [Online]. Available: https://swimlane.com/resources/ebook-automating-incident-response/

[2] I. Nedyalkov, A. Stefanov, and P. Apostolov, "Modeling of the convergence time of an IP - based network with different traffic loads," in *IEEE EUROCON 2019 -18th International Conference on Smart Technologies*. IEEE, jul 2019.

[3] *IGN MANTRA— Chairman, Peneliti Cyber War, Cyber Crime dan Cyber Security, Indonesia Academic CSIRT, Seminar Cyber Defence, Teknik lnformatika, Universitas Jendral Soedirman, PURWOKERTO, AcadlCSlR'l'.*

[4] I. academic CSIRT. Seminar cyber defence unsoed 21 september 2014. [Online]. Available: https://www.slideshare.net/-ignmantra/seminar-cyber-defence-unsoed-21-september-2014

[5] E. Paul van Kessel, *Cybersecurity regained: preparing to face cyber attacks 20th Global Information Security Survey 2 017–18*, 2018.

[6] E. Lichtblau, "Hackers Get Employee Records at Justice and Homeland Security Depts." 2 2016. [Online]. Available: https://www.nytimes.com/2016/02/09/us/hackers-access-employee-records-at-justice-and-homeland-security-depts.html

[7] Z. Zorz. (2016, 2) Info on 20,000 FBI and 9,000 DHS employees leaked following alleged DoJ hack - Help Net Security. [Online; accessed 10. Nov. 2019]. [Online]. Available: https://-www.helpnetsecurity.com/2016/02/09/info-on-20000-fbi-and-9000-dhs-employees-leaked-following-alleged-doj-hack

[8] C. Bing. Doe warns of potentially 'imminent' cyberattack on power grid. [Online]. Available: https://www.cyberscoop.com/-energy-department-warns-imminent-cyberattack-power-grid/

[9] S. Chapter IV: Ensuring Electricity System Reliability and Resilience, "Transforming the nation's electricity system: The second installment of the qer | january 2017."

[10] A. Mathur. (2019, 9) DXC Technology Co. (via Public) / Why predictable cyber security practices are less secure. [Online; accessed 1. Sep. 2019]. [Online]. Available: http://-www.publicnow.com/view/-6DE296A267A3EFD2290A46DC893EFB08836AB09F?2019-08-15-14:00:19+01:00-xxx2981

[11] M. Giles, "AI for cybersecurity is a hot new thing—and a dangerous gamble," *MIT Technology Review*, 8 2018. [Online]. Available: https://www.technologyreview.com/s/611860/ai-for-cybersecurity-is-a-hot-new-thing-and-a-dangerous-gamble

[12] ENISA, *Cyber Security Culture in organisations*, NOVEMBER 2017.

[13] L. Pietre-Cambacedes, M. Tritschler, and G. N. Ericsson, "Cybersecurity myths on power control systems: 21 misconceptions and false beliefs," *IEEE Transactions on Power Delivery*, vol. 26, no. 1, pp. 161–172, jan 2011.

[14] C. Gopalakrishnan, "Sophisticated tools provide false sense of cyber-security: Survey," 9 2019. [Online]. Available: https://www.scmagazineuk.com/sophisticated-tools-provide-false-sense-cyber-security-survey/article/1660872

[15] G. Ness. (2018, 5) The All or Nothing Cyber Security Paradox - Security Boulevard. [Online; accessed 3. Sep. 2019]. [Online]. Available: https://securityboulevard.com/2018/05/the-all-or-nothing-cyber-security-paradox

[16] W. Ashold. (2019, 9) Pen testers find weaknesses in banks' cyber security. [Online; accessed 3. Sep. 2019]. [Online]. Available: https://www.computerweekly.com/news/252441525/-Pen-testers-find-weaknesses-in-banks-cyber-security

[17] . Димитров, "Рискове при използване образи на виртуални машини в облака," *CIO*, Октомври 2013. [Online]. Available: http://cio.bg/-5745_riskove_pri_izpolzvane_obrazi_na_virtualni_mashini_v_oblaka&ref=cat

[18] C. S. Review. (2019, 2) Attack Uses Docker Containers To Hide, Persist, Plant Malware Cyber Security Review. [Online; accessed 21. Feb. 2019]. [Online]. Available: https://-www.cybersecurity-review.com/news-july-2017/attack-uses-docker-containers-to-hide-persist-plant-malware

[19] S. Sultan, I. Ahmad, and T. Dimitriou, "Container security: Issues, challenges, and the road ahead," *IEEE Access*, vol. 7, pp. 52976–52996, 2019.

[20] J. hua Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, dec 2018.

[21] S. Paavolainen and P. Nikander, "Security and privacy challenges and potential solutions for DLT based IoT systems," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, jun 2018.

[22] H. Halpin and M. Piekarska, "Introduction to security and privacy on the blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, apr 2017.

[23] M. Lagazio, N. Sherif, and M. Cushman, "A multi-level approach to understanding the impact of cyber crime on the financial sector," *Computers & Security*, vol. 45, pp. 58–74, sep 2014.

[24] T. Pham. (2016) A guide to stronger security in pci dss 3.2. [Online]. Available: https://duo.com/blog/a-guide-to-stronger-security-in-pci-dss-3-2

[25] "Data breach incident investigation report. cathay pacific airways. unauthorized access to personal data of passengers." Report Number : R19 -15281 Date Issued: 6 June 2019.

[26] F. S. B. C. P. G. Federal Communication Commission, *Cyber Security Planning Guide*, 2015.

[27] M. Hopkins and A. Dehghantanha, "Exploit kits: The production line of the cybercrime economy?" in *2015 Second International Conference on Information Security and Cyber Forensics (InfoSec)*. IEEE, nov 2015.

[28] M. Trend. (2017, 2) Tracking the Decline of Top Exploit Kits - TrendLabs Security Intelligence Blog. [Online; accessed 5. Sep. 2019]. [Online]. Available: https://blog.trendmicro.com/-trendlabs-security-intelligence/tracking-decline-top-exploit-kits

[29] V. Chebyshev, "IT threat evolution Q2 2018. Statistics," 12 2018. [Online]. Available: https://securelist.com/it-threat-evolution-q2-2018-statistics/87170

[30] T. smart security on demand, *The Security Survival Guide for Growing Businesses*, 2016.

[31] B. Li and J. C. C. T. Analysts). (Posted on:March 15, 2016 at 5:43 pm in:Exploits, Vulnerabilities) Exploit kits in 2015: Scale and distribution.

[32] (2019, 11) What Executives Get Wrong About Cybersecurity. [Online; accessed 10. Nov. 2019]. [Online]. Available: https://sloanreview.mit.edu/article/what-executives-get-wrong-about-cybersecurity

[33] L. Tucci. (2016, 5) Stuart Madnick: Dark Web hackers trump good guys in sharing information. [Online; accessed 10. Nov. 2019].

[34] K. Corbin. (CIO) U.s. cio aims to cut legacy spending, proposes it modernization. [Online]. Available: http://-www.cio.com/article/3075842/government-use-of-it/u-s-cio-aims-to-cut-legacy-spending-proposes-it-modernization.html