UDK: 316.42
316.77:004.773

Pregledni rad
Rad je primljen/ Received: 14.02.2022;
Prihvaćen/ Accepted: 18.04.2022

Siniša Franjić PhD,[1]
Independent Researcher, **R. Croatia**
JEL:K20

INTERNET AND MODERN INFORMATION TECHNOLOGY IN THE FUNCTION OF SOCIETY DEVELOPMENT

***Abstract**: The development of modern information technology has changed the world around us, but also the world within us. The Internet has begun to shape our development, behavior, and social norms that can be interpreted through phenomena related to technology and human behavior in virtual reality taking place on the Internet. This means that technology has a huge impact on everyday human life. When we talk about modern technologies, we often think only of smartphones, the Internet and social media as the main factors that have significantly changed our lives, social relations, but also health. And often they pay attention only to their negative sides. With good reason, because negative side effects are not uncommon.*
***Keywords**: Internet, Smart Electronics, Machine Learning, Cybercrime*

Introduction

In the last few decades, we have witnessed the rapid growth of the Internet, mobile technology and the correspondingly rapid growth of online crimes, or cybercrimes. With this growth, there has been a spike in the rate of cybercrimes committed over the Internet (Kizza, 2014). This has resulted into some people condemning the Internet and partner technologies as responsible for creating new crimes and the root causes of these crimes. However, there is hardly any new crime resulting from these new technologies. What has changed, as a result

[1] sinisa.franjic@gmail.com; https://orcid.org/0000-0002-9939-7671

of these new technologies, is the enabling environment. Technology is helping in the initiation and propagation of most known crimes. As we get rapid changes in technological advances, we are correspondingly witnessing waves of cybercrimes evolving.

We live in an analogue world and, increasingly, work, play and do business in a digital one (Calder, 2005). Our assets, the things we own in either world and that are valuable to us, are also attractive to others. As we've extended our field of activity into the digital world wide web (or internet), as we've developed new technologies and acquired new skills, so we've been followed by all those antisocial elements who plagued us in the analogue one.

Over the centuries, we've become accustomed (particularly in the First World) to taking appropriate precautions around our analogue assets, health and security. We know how to secure homes, offices and cars. We know what precautions to take while walking, shopping or doing business. We know which neighbourhoods to stay out of. We teach our children what to do, and we have well-developed police and justice systems that deal (to one extent or another) with miscreants.

Although the police and justice systems are still coming to grips with the digital world, the miscreants – criminals (of all sorts: organized, white collar and occasional), malefactors, spies and other undesirables – have already successfully adapted their modus operandi to cyberspace. Of course, that doesn't mean that they've deserted the analogue world, they've just extended their sphere of operations to the digital one. We've therefore got to get as good at dealing with the cyber threats and risks as we already are at dealing with the analogue ones.

The growth of computers and of information technology has been explosive (Bosworth et al., 2014). Never before has an entirely new technology been propagated around the world with such speed and with so great a penetration of virtually every human activity. Computers have brought vast benefits to fields as diverse as human genome studies, space exploration, artificial intelligence, and a host of applications from the trivial to the most life-enhancing.

Unfortunately, there is also a dark side to computers: They are used to design and build weapons of mass destruction as well as military aircraft, nuclear submarines, and reconnaissance space stations. The computer's role in formulating biologic and chemical

weapons, and in simulating their deployment, is one of its least auspicious uses.

Of somewhat lesser concern, computers used in financial applications, such as facilitating the purchase and sales of everything from matchsticks to mansions, and transferring trillions of dollars each day in electronic funds, are irresistible to miscreants; many of them see these activities as open invitations to fraud and theft. Computer systems, and their interconnecting networks, are also prey to vandals, malicious egotists, terrorists, and an array of individuals, groups, companies, and governments intent on using them to further their own ends, with total disregard for the effects on innocent victims. Besides these intentional attacks on computer systems, there are innumerable ways in which inadvertent errors can damage or destroy a computer's ability to perform its intended functions.

In a world of rapid socio-technical transformation and increasing fragmentation of political power and authority, cyber security has firmly established itself as one of the top national security issues of the 21st century (Wenger et al., 2022). Managing cyber insecurities will most likely further increase in complexity and political significance in the next decade, co-produced by an acceleration of the ongoing socio-technical transformations, on the one hand, and the changing dynamics of the related political responses, on the other.

The current state of cyber security politics is very much a reflection of the interplay between the underlying forces of great power competition and the dynamics of socio-technical and socio-economic globalization processes. From the interplay of these two processes emerge the two key factors – multidimensional uncertainty and socio-political ambiguity – that characterize the current context of cyber security politics at both the national and international levels. Multidimensional uncertainty plays a key role in the emergence of cyber insecurity as a wicked problem and shapes – and is shaped by – the ambiguity of cyber security politics.

Business Environment

The larger business environment is different from that of a small business in two ways: firstly, the majority of people using computers in the business do not actually own the computers, and so are unlikely to have an owner's interest in their security; and, secondly, the more complex the organization, the more likely it is to handle a greater range of business and information demands, to have a more complex computer infrastructure, to have exposure to a wider range of threats and to have more at risk (Calder, 2005).

There are, however, 14 basic information security principles that all organizations need to implement: the Infosec Basics for Business. They contain an organizational perspective on the essentials that are in the SOHO Internet Highway Code 2, and are designed to operate alongside that code. In other words, the Infosec Basics provide basic guidance on the minimum security standards that should be implemented in organizations of any size, and the Internet Highway Code can provide guidance for their employees on their role in the implementation of that strategy. Every organization should issue all their employees – and particularly employees who are teleworkers or mobile workers – with a copy of the Internet Highway Code alongside an organization-specific user agreement.

While the basics should be implemented in every business, they are only a starting point, not a final solution. A final solution will be the result of moving beyond the basics. All businesses should, once the basics are satisfactorily in place, assess the entire spectrum of threats and risks they face and implement controls that will deal adequately with them. Risk assessment is covered later in this chapter.

The Infosec Basics for Business are:

1. Have a policy.
2. Insist on accountability and responsibility.
3. Identify asset ownership and classification.
4. Address information security in contracts: all employment and third party contracts must include information security.
5. Provide for the physical security of information systems.
6. Have up-to-date anti-malware software.

[2]The SOHO Internet Highway Code provides guidance for the secure management of a standalone computer or a micro-network in a small office or home office.

7. Implement and enforce user access controls.
8. Implement and enforce system access controls.
9. Manage vulnerabilities.
10. Have an incident response process.
11. Have basic business continuity and disaster recovery plans.
12. Monitor compliance.
13. Document the essential policies, processes and procedures.
14. Ensure that users are trained and aware of their responsibilities.

All business investments require trade-offs between risk and reward (Kaplan et al. 2015). Does the interest rate on a new bond issue adequately compensate for the risk of default? Are the potential revenues from entering a new emerging market greater than the risk that the investments will be confiscated by a new regime? Does the value of oil extracted via deep-water, offshore drilling outweigh the chance of a catastrophic accident? Tough questions must be answered by weighing up the business imperatives against a calculation of the risk - and the greater the risk, the harder it is to make the case for investment.

Technology investments are no different. They, too, have always been a trade-off between risk and return. However, for enterprise technology, increased global connectivity is raising the stakes on both side of the equation. The commercial rewards from tapping into this connectivity are enormous, but the more tightly we are connected, the more vulnerabilities exist that attackers can exploit and the more damage they can do once inside. Therefore, when a manufacturer invests in a new product life-cycle management system, it is making a bet that the system will not enable the theft of valuable intellectual property. When a retailer invests in mobile commerce, it is betting that cyber-fraud won't critically damage profitability. When a bank invests in customer analytics, it is betting that the sensitive data it analyzes won't be stolen by cyber-criminals. The odds on all those bets appear to be shifting away from the institutions and toward cyber-attackers. They could swing decisively their way in the near future given most companies' siloed and reactive approach to cybersecurity.

GDPR

One of the most radical changes to affect organisations as a consequence of the GDPR (General Data Protection Regulation 2016/679) is the legal requirement that data protection must be 'baked' into an organisation's culture, systems and processes by design and default (Katz et al., 2020). To understand how the GDPR works in practice it is vital to understand these concepts.

Data protection by design means integrating data protection safeguards into organisations' data processing activities and business practices from the very beginning of a project life cycle. Although this concept is not new, the changes made by the GDPR mean that it is now a legal requirement.

Data security is no longer seen as an afterthought, but as a first priority at every stage of the process in order to minimise the risk of harm to individuals. But this philosophy is not just about reducing the risk to individuals, it also reduces the risk to data processing organisations. This is because it is much easier, and therefore cheaper, to put appropriate data security provisions in place from the start, than try to fix them further down the line.

Data protection by default, also known as 'data minimisation' or the 'privacy first' approach, concerns data collection. This model focuses on the idea that the amount of data that organisations capture should only ever be the bare minimum that is needed to achieve an objective. For example, data collection processes on an app should automatically be set to collect the minimum amount of data needed for the app to function. The user can then choose if they want to change the privacy settings to allow data to be captured and shared above the minimum level.

Smart Electronics

The future Internet will comprise not only millions of computing machines and software services but also billions of personal and professional devices, diminutive sensors and actuators, robots, and so on, and trillions of sentient, smart, and digitized objects (Raj et al. 2017). It is an overwhelmingly accepted fact that the fast-emerging and evolving Internet of Things (IoT) idea is definitely a strategic and highly impactful one to be decisively realized and passionately sustained with the smart adoption of the state-of-the-art information

communication technology (ICT) infrastructures, a bevy of cutting-edge technologies, composite and cognitive processes, versatile and integrated platforms, scores of enabling tools, pioneering patterns, and futuristic architectures. Industry professionals and academicians are constantly looking out for appropriate use and business and technical cases in order to confidently and cogently proclaim the transformational power of the IoT concept to the larger audience of worldwide executives, end users, entrepreneurs, evangelists, and engineers.

A growing array of open and industry standards are being formulated, framed, and polished by domain experts, industry consortiums, and standard bodies to make the IoT paradigm more visible, viable, and valuable. National governments across the globe are setting up special groups in order to come out with pragmatic strategies, policies, practices, and procedures to take forward the groundbreaking ideas of IoT, and to realize the strategic significance of the envisioned IoT era in conceiving, concretizing, and providing a set of next-generation citizen-centric services to ensure and enhance people's comfort, choice, care, and convenience. Research students, scholars, and scientists are working collaboratively toward identifying the implementation challenges and overcoming them through different means and ways, especially through standard technological solutions.

Our living, relaxing, and working environments are envisioned to be filled up with a variety of electronics including environment monitoring sensors, actuators, monitors, controllers, processors, tags, labels, stickers, dots, motes, stickers, projectors, displays, cameras, computers, communicators, appliances, robots, gateways, and high-definition IP TVs. Apart from these, all the physical and concrete items, articles, furniture, and packages will become empowered with computation and communication-enabled components by attaching specially made electronics onto them. Whenever we walk into such kinds of empowered and augmented environments lightened up with a legion of digitized objects, the devices we carry and even our e-clothes will enter into a calm yet logical collaboration mode and form wireless ad hoc networks with the inhabitants in that environment. For example, if someone wants to print a document in his or her smartphone or tablet, and if he or she enters into a room where a printer is situated, the smartphone will begin a conversation with the printer automatically and send the document to be printed.

Biometrics

Biometrics is an authentication system that uses the unique physical characteristics of each person to be authenticated by the IT system (Franjic, 2021). This means that when logging in to a computer, instead of entering a username and password, the user authenticates himself with something else that is unique to him and that makes him unique and different from other people. The most commonly used features are fingerprint, hand and face geometry, iris appearance etc. All of these characteristics are unique to each person. The application in criminalistics and forensics is very significant, especially in the part related to identification.

The term biometrics refers to the measurement of physical features of the human body (Smith, 2019). Put differently, biometrics is, '[t]he science of automatic identification or identity verification of individuals using [unique] physiological or behavioural characteristics'. It's an automated process that doesn't require another human being to make a comparison. Biometric systems can also function without active input, cooperation or even knowledge on the part of the subject.

With all the fascinating applications of this technology, it's no wonder that biometrics has been a source of inspiration for sci-fi movies and television for decades. Your iris scan unlocks the door of your house. Your fingerprint lets you into your office. In essence, you are your own key. Although biometrics may seem like the stuff of the future, it's actually the oldest form of identification. From a very young age, most humans can recognize a familiar face, voice or movement. When we recognize people, we recognize their physical features. Our ancestors used this type of authentication even before they fully evolved into humans.

Biometric security follows a standardized set of criteria – the so-called 'seven pillars' – by which to judge the suitability and efficacy of particular characteristics and systems. These include: (1) universality, i.e. that all humans share the characteristic, (2) distinctiveness, that for each person these features are unique to a significant degree and (3) permanence, that the characteristics are permanent and will remain largely unchanged throughout life. The

pillars also include standardized ratings according to (4) collectability, i.e. that the biometric may be efficiently collected, (5) performance, or the accuracy of matching, (6) acceptability, the acceptability of the system to users and finally, (7) security, the degree to which the system is open to circumvention or 'spoofing'. Some biometrics, such as fingerprints, rank very high; other biometrics may score well in terms of some of the pillars but not others.

Machine Learning

The large volume of data and information available on computers and the network has completely changed the direction of artificial intelligence (AI), thus influencing the ability of malicious software to invade systems and the consequent protection responses (Monteiro et al, 2022). It is in this context that Machine Learning emerges as one of the most promising ways of applying AI for the development of information security systems.

Capable of increasing productivity and operational efficiency, this technology has had an impact on the anti-fraud industry and reinforced current security solutions. Machine Learning presents itself as an application that allows systems to perform tasks that only people would be capable of.

Information security is an increasingly important issue for all organizations. The increase in cybercrime means that organizations increasingly need to invest in security as a way to protect themselves and ensure the protection not only of their internal information but also of their users' information, especially after the new data protection laws.

An essential ally in this process today is Machine Learning. Integrated with efficient information security policies, it becomes possible to significantly increase the protection of your business to avoid actions by hackers who want to usurp your data. Machine Learning is defined as the ability of computers to learn to perform tasks without having been explicitly programmed to do so. That is, using mathematical techniques on large data sets, the algorithms build behavioral models and use them as a basis to perform actions and make predictions based on new input data.

When present in a cybersecurity solution, Machine Learning can delve into the history of security data to create an image of a specific attack based on its variables and relationships and predict, based on that knowledge, the next attack.

Machine Learning is a way of creating AI from the collection and analysis of data, the results of which allow the machine to "learn" a particular task to perform it on its own or to be able to determine a future situation or information based on observed patterns. The premise is to basically recreate a pattern as complex as that of human intelligence, performing a series of tasks and learning at every moment. However, what has been achieved so far is the learning of specific tasks, the so-called limited AI. This is the case with algorithms that use data from a user to indicate films and music that could be of interest to them.

Machine learning lies at the core of many modern applications, extracting valuable information from data acquired from numerous sources (Muñoz-González et al., 2019). It has produced a disruptive change in society, providing new functionality, improved quality of life for users, e.g., through personalization, optimized use of resources, and the automation of many processes. However, machine learning systems can themselves be the targets of attackers, who might gain a significant advantage by exploiting the vulnerabilities of learning algorithms. Such attacks have already been reported in the wild in different application domains.

Advances in machine learning have produce a disruptive change in the society and the development of new technologies. In the Big Data era, an increasing number of services rely on AI and data-driven approaches that leverage the huge amount of data available from diverse sources, including people, devices, and sensors. Machine learning algorithms allow to extract valuable information from this overwhelming amount of data, providing powerful predictive capabilities. The use of machine learning facilitates the automation of many tasks, and brings important benefits in terms of new functionality, personalization, and optimization of resources.

Machine learning has been successfully applied in many different application domains, including computer and system security. Thus machine learning is at the core of most non-signature-based detection systems, including, among other things, spam,

malware, network intrusions, and fraudulent activities. In contrast to traditional signature-based systems, machine learning has generalization capabilities, i.e., learning algorithms can produce predictions for samples they have not seen before.

Despite the benefits of machine learning technologies, learning algorithms can be abused, providing new opportunities to cybercriminals to conduct illicit and highly profitable activities. It has been shown that machine learning algorithms are vulnerable and can be the objectives of attackers, who might gain a significant benefit by exploiting the vulnerabilities of these algorithms. In fact, machine learning itself can be the weakest link in the security chain, and its vulnerabilities can be exploited by attackers to compromise entire infrastructures. Attackers can inject malicious data to poison the learning process or manipulate data at test time, exploiting the blind spots and weaknesses of the learning algorithm to evade detection.

The prominence of artificial intelligence (AI) and specifically machine- and deep-learning (ML/DL) solutions has grown exponentially (Bosch et al., 2021). Because of the Big Data era, more data is available than ever before, and this data can be used for training ML/DL solutions. In parallel, progress in high-performance parallel hardware such as GPUs and FPGAs allows for training solutions of scales unfathomable even a decade ago. These two concurrent technology developments are at the heart of the rapid adoption of ML/DL solutions.

Virtually every company has an AI initiative ongoing and the number of experiments and prototypes in the industry is phenomenal. Although earlier the province of large Software-as-a-Service (SaaS) companies, our research shows democratization of AI and broad adoption across the entire industry, ranging from startups to large cyber-physical systems companies. ML solutions are deployed in telecommunications, healthcare, automotive, internet-of-things (IoT) as well as numerous other industries and we expect exponential growth in the number of deployments across society. As examples, ML solutions are used in the automotive industry to explore autonomous driving and as a means to increase efficiency and productivity. In domains such as e.g. mining, autonomous vehicles are currently being used in under-ground operations where human safety is a concern and in situations where there is a risk of accidents.

Similarly, self-driving trucks can operate largely automatically within e.g. harbor or airport areas which helps to increase both productivity and safety. In the defense domain, AI segmentation is used to identify buildings, roads, or any type of land at pixel level from a great height. Besides, AI technologies provide a range of opportunities in a fast-moving emergency where there is conflicting information and where there is a need to rapidly establish an understanding of the current situation, as well as for prediction of future events.

Defense

The defense problem presents many challenging requirements from both modeling and computational perspectives (Miehling et al., 2019). The problem is inherently dynamic, evolving over time as a function of the defender's actions and (potentially unobservable) events from the cyber environment. New information is continuously revealed to the defender as the problem evolves, all of which, in general, must be used in the defender's decision making process. The model for the cyber environment, termed the threat model, must be sufficiently expressive to describe the complex nature of attacks. In particular, attacks are progressive, consisting of multiple stages and involving the combination of many vulnerabilities across multiple network elements, and persistent, with attackers continuing to attempt to fulfill their objective, using various attack pathways, until they are successful. The defender, in its attempts to interfere with or mitigate attacks, must be aware of the conflicting effects of its defense decisions on the system. It is faced with an unavoidable tradeoff between security and availability; performing system modifications that lower an attack's chance of success also interfere with the normal functionality and usability of the system by trusted users. Beyond modeling challenges, the defense problem presents significant challenges from a computational perspective. The systems that are targeted by cyber attacks are large-scale, consisting of many hosts, each containing a wide-range of software and operated by a large collection of users. Reasoning about all possible ways such systems can be attacked often leads to a combinatorial explosion in complexity. As a result, scalable algorithms must be developed, often requiring approximations or novel solution techniques (such as

sampling methods or system decompositions). One must also ensure that algorithms are able to meet the strict timing requirements of the system by prescribing defense decisions quickly. Oftentimes, defense decisions have a limited window of usefulness; prescribing a defense decision too late can be as ineffective as taking no action at all.

Cybercrime

Computer crime is a form of criminal behavior in which the use of computer technology and information systems is manifested as a mode of crime or the computer is used as a means or purpose of perpetration with which is producing some relevant criminal consequence (Franjić, 2020). Computer crime is also an unlawful violation of property in which computer data is intentionally altered (manipulated by a computer), destroyed (computer sabotaged) or used in conjunction with hardware (theft of time).

The concept of cybercrime can be interpreted in many ways (Kosiński et al., 2021). Cybercrime can be understood in a narrow sense (computer crime) covering any illegal behaviour carried out by means of electronic activities aimed at the security of computer systems and the data processed therein. Cybercrime can also be understood in a broad sense (computer-related crime)—as any illegal behaviour committed through or in relation to a computer system or network, including offences such as the illegal possession, offering or dissemination of information through a computer system or network. Cybercrime in this sense ranges from economic crimes such as fraud, counterfeiting, industrial espionage, sabotage and extortion, to computer piracy and other crimes against intellectual property and breaches of privacy, promotion of illegal and harmful content, facilitation of prostitution and other crimes against morals, to organized crime. The latter border is also marked by cyber-terrorism, involving attacks on public security, life and electronic warfare against critical infrastructure. In the concept of cyber-terrorism, as in cybercrime, the prefix “cyber” refers to committing a crime involving new information technologies or using cyberspace for traditional activities (e.g. planning, communication, intelligence, logistical and financial activities).

It is generally accepted that cybercrime is one of the threats that includes unauthorized conduct aimed at accessing, acquiring, manipulating or losing the integrity, confidentiality and availability of data, applications or computer systems. Cyberthreats also include cyber-terrorism, cyber-spy and cyber warfare. Cyber-threats are considered in the context of cyber-security understood as the security of globally connected information systems (e.g. internet infrastructure), telecommunication networks, computer systems and industrial control systems. Cyber-security breaches are used for a wide range of criminal activities that cause significant material and non-material damage to organisations, companies and individuals. It cannot be overlooked that this is an important problem also in the context of internal security and thus also state security.

Forensics

We turn to forensics when it's necessary to investigate activity on a system (Shema, 2014). Logfiles do not always capture information relevant to answering questions. They may capture data like "When and from what IP address did a user access a system?" but may not be able to answer questions like "What files have been executed or deleted?" or "Were these files accessed when the user logged in?" We need tools and techniques to recover or deduce this kind of information, especially if logfiles have been erased by an attacker trying to cover their tracks.

The activity under investigation need not be malicious or illegal. It may be related to violations of corporate policy (such as viewing and downloading porn on a corporate system, or sending harassing e-mails). One important facet of computer forensics is the legal aspect of collecting evidence, maintaining a chain of custody, and working with law enforcement.

Forensics focuses as much on the temporal characteristics of an event as it does on the sources and targets associated with it. An investigator may spend a lot of effort piecing together a timeline of events in order to build a story of what happened. The order in which systems were compromised may indicate an attack vector (earlier systems may have been compromised by software exploits, while later systems may have been accessed by compromised credentials). Or, the

order of events may indicate an attacker's motivation or level of sophistication. It's important not to overanalyze events and ascribe more characteristics than evidence supports, but such evidence should help inform levels of confidence in defining an attacker or comparing them to other events.

Two broad categories of information to collect are volatile data and nonvolatile data. Volatile data typically covers anything that disappears when you turn off or restart a system. For example, you'll lose the list of currently running processes; possible clues within the system's memory will disappear; and network connections that might indicate an attacker's origin or their next target will be lost. This kind of information can provide clear indicators of activity when you can directly view a suspicious process or user access.

Nonvolatile data typically covers anything that remains static (or relatively so) even when a system is not running. The system's drive is the most obvious example. Deleted files remain on the drive even if they no longer appear in the file system. This category could also cover more specific files, like browser caches or the Windows Registry.

It's important to have an incident response procedure in place that instructs investigators on what to collect and how to collect it. This way they do not lose volatile data, forget to copy log files, or make trivial mistakes when dealing with suspicious activity on a system.

Conclusion

The technological age we are in has brought many novelties in a wide range. Technology has improved medicine, industry, science, which significantly affects everyday life. Technological progress and investment in new technologies are undoubtedly one of the factors of economic growth. Investments in Internet technologies in the public and private sectors must be increased, but also adjusted to the requirements of legislation on security and encryption. The low level of penetration of new technologies, as one of the most important generators of economic growth, is a consequence of political and economic barriers and dualisms that govern society and the economy.

References

1. Bosch, J.; Olsson, H. H.; Crnkovic, I. (2021). Engineering AI Systems: A Research Agenda in Luhach, A. K.; Elçi, A. (eds) *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*, IGI Global, Hershey, USA, pp. 1. - 2.
2. Bosworth, S.; Jacobson, R. V. (2014). Brief History and Mission of Information System Security in Bosworth, S.; Kabay, M. E.; Whyne, E. (eds) *Computer Security Handbook, Sixth Edition*, John Wiley & Sons, Inc., Hoboken, USA, pp. 1*1. - 1*2.
3. Calder, A. (2005). *A Business Guide to Information Security - How to Protect Your Company's IT Assets, Reduce Risks and Understand the Law*, Kogan Page Limited, London, UK, pp. 1.; 16. - 17.
4. Franjic, S. (2021). Biometrics in Criminalistics and Forensics. *Int J Forensic Sci*. 3: 10-16.
5. Franjić, S. (2020). Cybercrime is Very Dangerous Form of Criminal Behavior and Cybersecurity, *Emerging Science Journal, Vol. 4., Special Issue "Internet of Things, Internet of Vehicles,, and Blockchain"*, Reggio Calabria, Italy, pp. 18. – 26., DOI: http://dx.doi.org/10.28991/esj-2020-SP1-02
6. Kaplan, J. M.; Bauley, T.; Rezek, C.; O'Halloran, D.; Marcus, A. (2015). *Beyond Cybersecurity - Protecting Your Digital Business*, John Wiley & Sons, Inc., Hoboken, USA, pp. 1. - 2.
7. Katz, A.; MacDonald, M.; Astley, T.; Guness, U.; Svorc, J.; McCormick, C. (2020). Data Protection in Practice in Holt, J.; Newton, J. (eds) *A Practical Guide to IT Law, Third Edition*, BCS Learning and Development Ltd, Swindon, UK, pp. 116. - 117.
8. Kizza, J. M. (2014). *Computer Network Security and Cyber Ethics, Fourth Edition*, McFarland & Company, Inc., Publishers, Jefferson, USA, pp. 3.
9. Kosiński, J.; Krasnodębski, G. (2021). Cybercrime Predicting in the Light of Police Statistics in Jahankhani, H.; Jamal, A.; Lawson, S. (eds) *Cybersecurity, Privacy and Freedom Protection in the Connected World - Proceedings of the 13th International Conference on Global Security, Safety and Sustainability, London, January 2021*, Springer Nature Switzerland AG, Cham, Switzerland, pp. 55. - 56

10. Miehling, E.; Rasouli, M.; Teneketzis, D. (2019). Control-Theoretic Approaches to Cyber-Security in Jajodia, S.; Cybenko, G.; Liu, P.; Wang, C.; Wellman, M. (eds) *Adversarial and Uncertain Reasoning for Adaptive Cyber Defense - Control- and Game-Theoretic Approaches to Cyber Security*, Springer Nature Switzerland AG, Cham, Switzerland, pp. 12. - 14.
11. Monteiro, A. C. B.; França, R. P.; Arthur, R.; Iano, Y. (2022). The Fundamentals and Potential for Cyber Security of Machine Learning in the Modern World in Kaushik, K.; Tayal, S.; Bhardwaj, A.; Kumar, M. (eds) *Advanced Smart Computing Technologies in Cybersecurity and Forensics*, CRC Press, Taylor & Francis Group, LLC, Boca Raton, USA, pp. 120. - 121.
12. Muñoz-González, L.; Lupu, E. C. (2019). The Security of Machine Learning Systems in Sikos, L. F. (ed) *AI in Cybersecurity*, Springer Nature Switzerland AG, Cham, Switzerland, pp. 47. - 48.
13. Raj, P.; Raman, A. C. (2017). *Abusing the Internet of Things - Enabling Technologies, Platforms, and Use Cases*, CRC Press, Taylor & Francis Group, Boca Raton, USA, pp. 1. - 3.
14. Shema, M. (2014) *Anti-Hacker Tool Kit, Fourth Edition*, McGraw-Hill Education, New York, USA, pp. 534.
15. Smyth, S. M. (2019). *Biometrics, Surveillance and the Law - Societies of Restricted Access, Discipline and Control*, Routledge, Taylor & Francis Group, Abingdon, UK, pp. 21. - 23.
16. Wenger, A.; Cavelty, M. D. (2022) Conclusion: The Ambiguity of Cyber Security Politics in the Context of Multidimensional Uncertainty in Cavelty, M. D.; Wenger, A. (eds) *Cyber Security Politics - Socio-Technological Transformations and Political Fragmentation*, Routledge, Taylor & Francis Group, Abingdon, UK, pp. 239.

ИНТЕРНЕТ И САВРЕМЕНА ИНФОРМАЦИОНА ТЕХНОЛОГИЈА У ФУНКЦИЈИ РАЗВОЈА ДРУШТВА

Sažetak: *Razvoj savremene informacione tehnologije promenio je svet oko nas, ali i svet u nama. Internet je počeo da oblikuje naš razvoj, ponašanje i društvene norme koje se mogu tumačiti kroz fenomene vezane za tehnologiju i ljudsko ponašanje u virtuelnoj*

stvarnosti, koji se odvijaju na internetu. To znači da tehnologija ima ogroman uticaj na svakodnevni ljudski život. Kada govorimo o savremenim tehnologijama, često razmišljamo samo o pametnim telefonima, internetu i društvenim medijima kao o glavnim faktorima koji su značajno promenili naše živote, društvene odnose, ali i zdravlje. I često obraćaju pažnju samo na svoje negativne strane. Sa dobrim razlogom, jer negativne nuspojave nisu retkost.

***Ključne reči**: Internet, Pametna elektronika, Mašinsko učenje, Sajber kriminal.*

Kako citirati ovaj članak/how to cite this article:
Franjić, S. (2022) Internet and modern information technology in the function of society development. *Horizonti menadžmenta*. II (1), 35-52