High-Tech Criminality

MILICA D. ĐEKIĆ, Subotica

Professional Paper
UDC: 343.533::004
DOI: 10.5937/tehnika2106865D

Abstract: Cybercrime is an activity that originates from a hacker's workstation, spreads through the web and affects the endpoint infrastructure. From a professional point of view, it's one of the most requiring criminologist cases in all crime areas, because it needs a plenty of skill to be recognized, managed and resolved. The modern global landscape shows a certain tendency of not being capable to respond to such a security challenge. In other words, the cyber criminals are well-motivated and work for a high profit, so it's obvious why that branch of criminality cannot be fully covered at present. Indeed, we need much better capacities to tackle such a concern and as the entire world suffers so obvious cyber skill shortage it's clear why we are dealing in maze. In this paper, we discuss high-tech crime as a social, economical and above all; security challenge trying to indicate some recommendations that could provide us a deeper understanding of the topic.

Key Words: *high-tech crime, cyber defense, intelligence, technology, strategy*

1. INTRODUCTION

The criminality is a very complex term affecting physical, virtual and mental health's performances. The crime as we know it today had been recognized with the application of the first laws that had suggested what was allowed to do and what took with itself a punishment. The fear from being sanctioned has made many people throughout history to choose a life and work according to the legal frameworks as there have always been a lot of so to lose. The societies with the weak defense systems can become an oasis for the criminals and terrorists. The reason for so is many of them would commit a crime and just avoid the punishment, so the criminality will spread as some transferrable disease similarly as a pandemic of some illness. In other words, those communities need to be treated carefully as the pandemic does not know the borders and always can reflect to its surrounding as well as much wider. With a nowadays shift into a cyber environment the crime has begun happening at some far more sophisticated level. In other words, anyone with a device being connected to the web can become a victim of the high-tech criminality. That sort of the crime is hard to investigate as it seeks something so demanding and that is a skill. Also, the problem is the lack of the ongoing legal regulations that would recognize any possible incident and predict an adequate sanction for so. In other words, we are yet far from being cyber safe.

The aim of the high-tech crime is to make harm to the existing IT resources and those sorts of the operations can cause the serious mental health's conditions to victims of the crime. For instance, in a business world the people are limited with their tasks' deadlines and if they use cyberspace to obtain so it could be so frustrating to face up a cyber attack that would provide some sort of a work discontinuity and eventual loss of sensitive data. IT security professionals apply a backup in such a sense, but it can be quite trickery to return everything into normal.

Sometimes the cyber campaigns could be correlated with the psychological operations and in that case the victims could suffer some negative emotions such as fear, anxiety or tension. If our organism is overwhelmed with those sorts of feelings a person can become irrational putting aside his logics and problem-solving skills that are usually typical for rational and critical thinking minds. The fear can paralyze our capacities to respond and leave us being fully hopeless in front of so merciless predators. Exactly that's the point of the cyber-led psychological operation to make everyone being affected and helpless in front of the cybercrime underworld. The internet is an astonishing communication medium and it's clear why the impacts

Author's address: Milica Đekić, Vase Pelagića 39, Subotica
e-mail: milicadjekic82@gmail.com

Paper received: 27.10.2021.
Paper accepted: 22.11.2021.

of losing the connection could be so threatening to all its clients.

The development and deployment of the computers, internet and the other digital systems have begun with the 3rd industrial revolution. That's basically a time when the very first laws against the cybercrime have been made. The first cyber acts have appeared in the United States as that country has recognized the problem with that time's technologies and lately the entire world just coped with such a tendency. At the present, there are the billions of web connections across the globe, but yet too many countries struggle to adopt the ongoing legal regulations, best practices and the other things that give legality to the investigation to be conducted. In the majority of societies with the well-developed laws against the high-tech crime it's a challenge to manage such a case for a reason there is so obvious need for procedures, policies and evidence collecting processes that can offer a deep investigation and a fair conclusion of the case. At every single moment, there are the thousands of cyber incidents in the world. Many of them have never been reported and probably the message of the high-tech syndicate is either we will tolerate cyber attacks or let the IT pirating being fully legal. From criminology's point of view, that's a classical blackmail and the demand for the cyber industry of the future is to produce much more superior solutions that will in cooperation with the active law enforcement be capable to show to those guys the justice.

2. WHAT IS A CYBERCRIME?

The high-tech crime employs people, technology and skill to commit an offense. That offense is normally under the Criminal Code and it's seen as criminality. The reason why cybercrime includes the people is someone must conduct the entire operation using the technology. That's not feasible if the actors do not have mastered the certain skills. The skills come with experience and it takes time to produce a comparable hacker. The age when the cyber criminals have the first contacts with the hacking is usually adolescence. The teenagers might begin to hack their teachers even in the high school. That's a big concern, because someone from the outside will encourage those young individuals to break the law. In other words, the experienced criminals will recruit so unaware youth to become the hackers and those mentors will advise the high-school students to go against their authorities. Some of the young people can see the cybercrime as a way to become independent from their parents as such a business can bring them a good income. The typical adolescent might be the rebel about anything and that sort of the revolt can be directed mainly to anyone who wants to gain an authority over their lives, actions and activities. Practically, the criminology suggests that could be a psychological trigger to many young people to get legal troubles as they feel they can make everything at that age and the money is only a suitable method to receive all they ever wanted. In other words, it's about their personal freedom and intent to move the barriers. The legal life has many limitations because it must be inside the frame, while the crime can offer unforgettable moments and life from someone's dreams. That is especially the case in the low-ranked law enforcement communities where the Police are weak and incapable to adequately respond to such a kind of the security challenge.

The way how the experienced cyber criminals recruit their apprentices is commonly via the Darknet communication systems, hacker's forums and discussion groups. The young persons are curious about what they can get making the next click, so they will easily accept a chat with the unknown individual. At the first glance, everything appears as so innocent and naive as it is so convenient exchanging the messages from so comfortable bedroom in some urban area of the world. Surfing the web is not a benign experience as there are so many people with more or less severe intents. To continue, once the teenager accepts the hacker for his contact he could get a business opportunity to join such a cyber gang. The criminology suggests that there is an entire procedure of receiving the new member in the team as those persons must be confirmed in order to any kind of the suspicion has been removed. In the Police jargon, they will certify their rookies before they give them an access to the organization and afterward the payment regarding their contribution to the tasks. In other words, the criminals must be sure that no one dealing with them is a threat to their business and saying in freedom. So simply, anyone with the bounty will be easily conquered and made to obey anything his bosses want from him. That's how new and new threats will be generated and the innocent kid's game in the school's computer lab will become someone's occupation for a life. The hacker's tools are available online and especially on the cybercrime websites, forums and chat rooms mainly being hidden on the Darknet. Once those young guys get into such a network they will become bad and as time goes on they will be worse and worse. The Police officers would say they will get a huge record from authorities.

3. WAYS TO IMPLEMENT STRATEGIES

As we have said, the majority of the countries worldwide do not cope with the adequate response to the cybercrime. The well-defined legal regulation can decrease a percentage of the high-tech crime somewhere as such a move could be a good prevention to the possible coming attempts. For instance, the cybercrime marketplace indicates there is a brand-new form of the malware being called the ransomware. That malicious code has affected the millions of devices over the globe since its very first versions and it is well-known as a blackmail tool that locks data and devices, then countdowns the time, seeking from the end user to pay a fee in return for his asset's liberation. The payment is done electronically via some bank card or Bitcoin cryptocurrency. The main targets of that malware are the large-scale businesses that cannot accept a work discontinuity and they will rather choose to pay for racketeering than to lose their time and money fixing the problem. The good strategy in such a sense could be to investigate such an incident spot, run a case and after arresting the criminals put the entire procedure into legal regulation seeking a strong punishment for those who committed such a crime. The cybercrime can be so annoying, but if we have in mind that it's very expensive it's clear why the response must exist and why it should be effective and much stronger.

4. TECHNOLOGICAL RESPONSE

The appropriate technological response can come from a cyber industry which task is to produce novel solutions that might offer a certain degree of security in the cyberspace. The good solutions are not the cheap ones and someone who invests into cyber defense must know that he might pay a lot. Also, the people who are good with finances will know how to reduce the expanses making a cost-effective plan for their organization. Indeed, the web is overwhelmed with the open-source and freeware software, so those applications can serve for, say, small and startup businesses that still need to get positioned on the marketplace. The high-tech criminality is so alarming activity and only with the good cyber defense it is possible to respond to such a challenge. The bad guys standing behind those operations are merciless professionals with more or less unhealthy life's habits who are capable and literally, daring to do anything for the profit. In other words, that kind of the behavior must be sanctioned and the authorities worldwide should develop much better capacities that will serve for a betterment of all.

5. LESSONS WE HAVE LEARNED

In our opinion, we live in an era of the cybercrime awareness attempts and practically we have learned a very few lessons from our current experience. It seems no one seriously opened the Pandora's Box as we yet deal with concerns, not solutions. In other words, everyone will talk about the cyber, but no one will take so dramatical actions that can save the world from that sort of the threat. Once we fill the skill gap the situation can become somewhat better, but even then it's hard managing a risk at an acceptable level.

6. IMPACTS TO SOCIETY

The high-tech crime costs the global economy trillions of dollars per an annum. Those are estimated results, while many believe that the consequences are far more dramatic. The internet is assumed as a critical infrastructure and its missing can catastrophically impact the entire countries and their nations. Indeed, talking about the cybercrime is not the matter of the media's stories as there should be taken much serious actions in order to combat that criminality. At the moment, only the very few countries in the world give promising signals, while the rest still waits for someone to wake them up. Apparently, the socio-economical impacts to communities are more than critical and if we do not raise awareness fully and do not take so powerful actions we can expect a crisis in the virtual environment that can affect both – our physical lives and businesses.

7. DISCUSSIONS

This effort has given a comprehensive overview of the current tendency in the virtual domain. The fast shift from physical to virtual surrounding has made a significant change of everything we have known before. The high-tech criminality is so dangerous area of the crime and with the prospective technological development it is expected that it could represent a big threat to lives of many. The sophisticated malware is one more splinter in our eye that drives us mad. The web is a huge collection of the content being visible or with the Darknet, so it's important to understand that sort of the concept before we make a decision to prepare our response to the cybercrime underworld and who knows – one day send them to the history.

8. CONCLUSION

The ongoing technological boom has made us being dependable on emerging technologies. For example, someone working in the office spends at least 8 hours per day over a business week in front of the screen. Basically, that's the minimum and we call those people the professionals. The stories that several hours per a day on the computer can cause an addiction do not make sense. The high-tech gangsters can obtain much more and as the role of the security is to be at least a step ahead of the threat the entire situation over the globe requires so deep approach to be tackled.

9. ACKNOLEDGEMENTS

Milica is so deeply grateful to her family for all their love, care and support through her life, education and career.

REFERENCES:

[1] Đekic M. The Internet of Things: Concept, Applications and Security, LAP Lambert Academic Publishing, 2017.

[2] Đekić M. The Insider's Threats: Operational, Tactical and Strategic Perspective, LAP Lambert Academic Publishing, 2021.

REZIME

VISOKOTEHNOLOŠKI KRIMINALITET

Informacioni kriminal je aktivnost koja započinje u hakerskoj radnoj stanici, širi se internetom i obuhvata krajnje tačke infrastrukture. Sa stručne tačke gledišta, to je jedan od najzahtevnijih kriminoloških slučajeva, jer podrazumeva mnogo znanja i veštine, kako bi bio prepoznat, kordinisan i rešen. Savremeno globalno obzorje beleži tendenciju nemogućnosti da odgovori na taj bezbednosni izazov. Drugim rečima, visokotehnološki kriminalci su dobro motivisani i rade za veliki profit, te je stoga jasno zašto taj vid zločina trenutno ne može da bude u potpunosti pokriven. Zaista, potrebni su mnogo bolji kapaciteti za borbu protiv tog kriminaliteta, a kako je u pitanju deficitarno zanimanje jasno je zašto tumaramo u lavirintu. U ovom radu, diskutujemo visokotehnološki kriminal kao društveni, ekonomski i iznad svega, bezbedonosni izazov pokušavajući da damo neke preporuke koje bi nam omogućile dublje razumevanje temetike.

Ključne reči: *visokotehnološki kriminal, bezbednost, saznanja, tehnologija, strategija*