

How to Combat a Terrorist Attack Using Modern Communications

By Milica D. Djekic

Combating the terrorist attack is a challenge for security, safety and community. Through the previous period of time we are witnessing the different types of terrorist offenses and those occurrences could teach us to take the active role in fighting against such a security issue. The modern defense doctrine would appoint us to observe the terrorist activities as the incidents happening on the battlefield as well as within some populated areas. The terrorists would target the places with so many people as the impacts of their actions would get so spectacular. They would believe that more people get affected with their operations; the easier they would spread the fear, panic and hesitating within the societies. At this stage, we would notice that the current terrorist incident within the urban areas could get characterized as guerilla attacks usually including the lone wolves operations. Once the terrorist incident happens, it's so important to resolve such a crisis at the crime scene. Sometimes the authorities cannot save the human lives and in those cases – the bad guys are getting the battle. If we talk about the hostage situations, we frequently need a team of the experienced Special Forces persons who are capable to tackle such a scenario and negotiate with the malicious actors. The question here would be if we could prevent the terrorist activities anyhow. The answer to this question is quite clear and it would suggest that there are the methods, techniques and strategies to maintain the risk from terrorism at the quite acceptable level. The near past experiences would indicate to us what the possible targets of the bad guys are and the entire defense and intelligence community would cope with the situation on the terrain from hour to hour. The role of this effort is to provide the better insight how the terrorist plans could get discovered in the practice and how we could potentially prevent any serious losses within our communities.

So, we would suggest that there are the ways to monitor the situation constantly and continuously and probably respond to any terrorist attack attempt. First, we need to realize that the terrorist groups are vitally dependable from the emerging communications technologies and if you want to get some of those actors, you need to cut on their information exchange. So many dedicated individual from a defense sector would work day by day and spend a lot of sleepless nights in order to protect the values of our ongoing civilization. That's not the easy task at all and such a profession seeks a lot of patience and

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

concentration in order to remain focused on your mission. The fact is defense forces would try to prevent the terrorist attacks putting under a control the entire cyberspace and the rest of the communications channels. Why it matters to do a surveillance of the web, phone lines and so many connected devices? The answer to this concern is quite obvious and it would indicate that those places got so busy and if you put them under the monitoring – you would undoubtedly find something. The experience would suggest that the bad guys would choose to frequent spots to operate and either they do something in the public or from the safe locations using their computers with the internet connectivity – they would get capable to exchange a plenty of information and make some plans on. The role of the defense persons is to discover such a communication and prevent any malicious stuff happens. The point is the good guys would deal with the technology that would provide them a chance to manage the risk at the quite good stage.

The fact is so many terrorist incidents would get discovered before anyone tries to do anything and from time to time the terrorists would succeed in their intent to cause harm to innocent civilians. Unfortunately, the defense community would sometimes fail to protect the people from those malicious operations and the entire societies would get wounded with those occurrences. The systems for the communications surveillance could get manual, semi-manual and fully automatic requiring more or less human engagement. Anyhow, the role of the defense professionals could not get underestimated in any fashion, because they would need to serve those technological advancements. The crucially important thing to such a task is the skill. In other words, if we need anyone preventing us from any crime – it's so significant to understand that such a person should get trained for that job. So many role-based systems would offer us an opportunity to do the administration of the user's accounts and monitoring such a communication – we would be in position to search for the possible malicious activities. The good instance of the role-based system is a Tor and if we want to make a deep dive into the Dark net, we would need to invest a lot of time and effort in order to analyze those communications. Also, if we use the modern technologies to prevent some kind of terrorist incidents, we should get aware of that such an approach could demand from us to search area by area attempting to figure out what is going on in some neighborhood. In addition, it's well-known that the majority of the international phone conversations are monitored and recorded by the authorities, so it's quite obvious that such a methodology could offer us the quite sati factionary results in preventing the both – crime and terrorism.

At this stage of our technological development – we are in position to take the advantage over the new technologies in order to prevent a lot of potentially malicious incidents. Combating the terrorism is the challenge as we have suggested at the beginning and we are quite confident that the coming technological solutions would offer us nearly limitless options to cope with such a concern. In other words, anyone wishing to commit the crime or organize the terrorist attack should think twice for a reason that sooner or later there will be the time to pay the big price on. The terrorism is the challenge and that's the fact, but would it be worth to take a part into such an adventure? We know that the people doing such a criminality would get led by some beliefs and in our opinion, it's so important to educate the human community how to deal with the highest values and standards. It's not that hard as it may appear at the first glance!

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About The Author



Milica D. Djekic is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book "The Internet of Things: Concept, Applications and Security" being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2019. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



The Challenges of Endpoint Security

By Milica D. Djekic

The endpoint devices are those gadgets that would be the part of a big computing network dealing with the endpoints as its final destinations. The endpoints computing units could be capable to send and receive the information packets once they are connected to the web. Also, if we talk about the ordinary network traffic – those devices could get able to conduct the similar operations, so far. All data being stored on the endpoint spots should meet the certain security procedures and policies. In so many cases, the endpoint computers would serve to the end users and either they are simply with the internet connectivity or any network connection – they would need some suggestions to get protected from cybercrime and the other hacker's operations. In other words, when we talk about the endpoints – we would mean by that the computers with the web connectivity that would cope with some IP addresses and get some data and applications being the part of their storage. It's quite obvious that anything being exposed to the internet could deal with some kind of cyber breach, so in such a case – we need to do a lot to secure our final destinations from those scenarios. In the practice, so many IT security experts would agree that the cyber breach is something being so inevitable and the best way to cope with such a situation is to apply the tools that would provide you an option to detect the breach. In addition, there are some best practice advices how to secure your data being on the endpoint device. The fact is so many computing networks would use the firewalls and the other protections, so the signal coming to the endpoints could get assumed as quite reliable. On the other hand, the hacker's incidents are not the rare case, so it's quite important to think hard how to tackle that sort of the risk.

The endpoint spots being connected to the internet would deal with their own IP addresses and once the hackers get how to find the certain device – they may try to start exploiting its vulnerabilities. The encryption at the endpoint places is from the vital significance if we want to protect our sensitive information. There are suggestions that the cyber breaches should get accepted as our reality and the huge question here is how we could cope with any data recovery and business continuity strategies. The quite trickery situation is if your endpoint spot got the target of cyber criminals and if you literally got so annoying hacker inside your system. In such a case, it's so important to take into consideration how to deliver the incident response being the key pillar of your cyber defense. In other word, maintaining the risk within your endpoints could get the quite complicated task, so our tip here is that you need so skillful cybersecurity professionals who would get well-trained in order to overcome all those challenges.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

Providing the security to the network's end users is the serious business, so we would recommend to anyone being with such a task to think smart in order to protect us from any kind of disadvantages. The endpoint security is not the job for amateurs and it seeks a huge knowledge that could support the IT security practitioner and his team to respond so actively to the wide spectrum of so different situations. The point is that there is no the real prevention in case of endpoint systems and what we can do only is the risk management. The people may believe that the endpoints are less important in the entire security practice, but sometimes they may appear as so strategically important places.

Through this effort, we would indicate it's the challenge protecting the endpoints and the fact is you need to deal with all three aspects of cyber defense being prevention, monitoring and incident response if you want to adequately cope with such a task. In our opinion, investing into IT infrastructure capacities could be the good decision, because your network's asset could provide the quite qualitative and safe web traffic to the end users. Also, there are a plenty of methods to discover someone's device being the part of the global network and then you should attempt to think like a hacker in order to realize what got uncovered within your infrastructure and at the next stage, you should think a bit as a cyber professional who is capable to cover the uncovered pieces of the situation. The reality would suggest that some parts of the cyberspace could get chronically uncovered and you would need to cover them on again and again in order to manage your risk. No problem could get resolved over the night and the purpose of cyber defense staffs is to get on a duty day by day, night by night with the task to tackle any single concern coming on. Even within some business your employees would rely on the endpoint systems and in such a case if their computers collapse – you should need to assure the regular backuping of their data. We would also mention that some of the files being on the endpoint machines should get encrypted in order to provide the lower level of the risk in case someone gets the idea to compromise them. The hackers would so clearly see all these vulnerabilities and they would know how to take advantage over your unprotected details, so if you are chronically the target to the cybercrime operations – you should know that the incident response solutions with the option to terminate someone's connection to your endpoint machine could get the right choice.

Finally, we should see that the endpoint security is so time consuming and it needs a lot of effort to get invested into the entire process of its cyber defense. The main point in this effort is that maybe we could try to apply a bit different point of view in terms of security and begin observing the things from the perspective of something being uncovered or vulnerable and try to figure out how such a weakness could get covered on. Once we cover our weakness – we would get less sensitive to the potential attacks or in other words, more resilient in any manner. In conclusion, cybersecurity as any defense is about the good covering on and if we master that practice, we would get in position to maintain the balance between the forces of offence and defense.

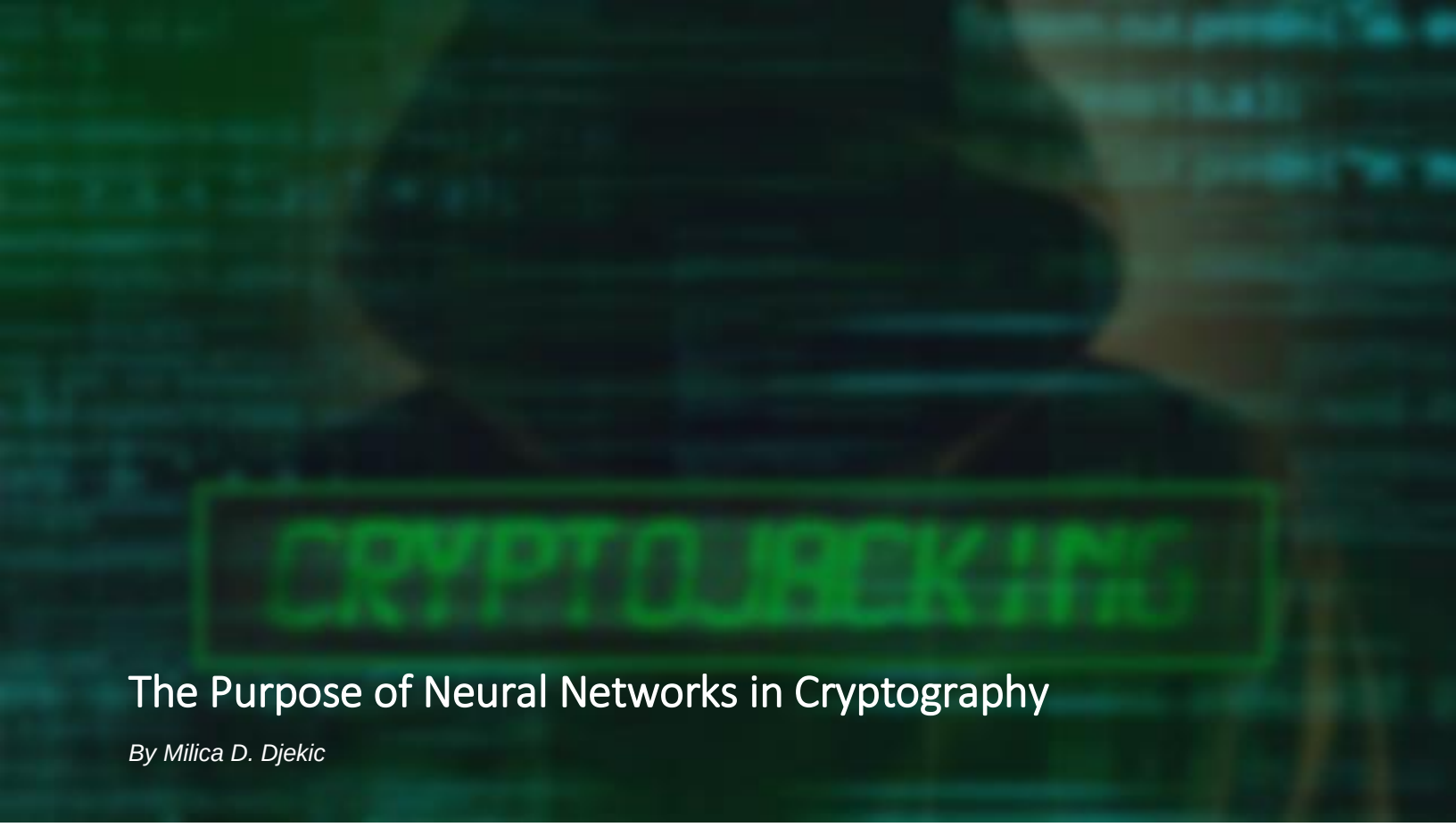
Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About The Author



Milica D. Djekic is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book "The Internet of Things: Concept, Applications and Security" being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel and Cyber Security Summit Europe being held in 2016 as well as CyberCentral Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2019. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide



The Purpose of Neural Networks in Cryptography

By Milica D. Djekic

Through the entire history of the Human Kind, the nature would keep surprising and surprising us with its wonders. So many beings on our planet got the capacity to learn and absorb the new knowledge and techniques. On the other hand, so many scientists would suggest that the humans got the best possible learning curve amongst all living things. In other words, we would get something the psychologist would call the intelligence. It's our ability to connect the stuffs with each other and do some reasoning about our surrounding. Apparently, the entire scientific community would recognize such a capacity with so many living beings and there would appear the need to mimic the nature in order to produce some technological solutions that would get the characteristics of the intelligent creatures. Here how we come to the term artificial intelligence or AI being the good representation of the natural intelligence. Moreover, it's quite clear that the AI projects would need the teams of the multidisciplinary experts and researchers, so if we want to use some inspiration coming from the natural phenomena – we would need to get familiar with so many fields of science and technology. The greatest challenge to the modern cognitive science is how human nervous system works and there are still a lot of questions in such an area that seek the rational answers and explanations. One of the biggest mysteries in the world is the human brain and many scientists believe that such a mechanism could provide us a deep understanding of the entire nature. At this stage of our development, we would know something about how the neurons function and as time goes on our perspectives will change and we would get some kind of the better situational awareness. So, the basic building block of our brains is the neuron and in case of the AI – the researchers would attempt to mimic how it works.

The fact is the human nervous system would use the electricity to transmit the signals through the human body. All the information from the body's peripherals would go to the brain and that organ would process any of those electrical signals. Every neuron would simply deal with its activation potential being the electrical impulse that would trigger the entire process of thinking, feeling and judging. The quite complicated, right? Practically, the human organism would transfer the time changing electrical impulses through itself and such electricity would cause the existence of the magnetic field making the huge electromagnetic field around our bodies. The majority of biological systems would cope with that sort of

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

bio-electromagnetic field and there are a lot of branches of science and technologies that would suggest to us we do not completely understand the life's processes within our environment. As we have indicated – the emerging technologies would try to cope with the biological systems intending to create something being capable to mimic the life. The human intelligence is quite complex to get simulated and the experience would suggest that there are still a lot of things that need to get resolved. At this stage, we would notice some progress in such a research and we would be at the beginning of the new exciting epoch in science and technology being recognized as the AI. The AI would rely on the findings coming from neural science and it would try to deal with the well-known theories of the human mind. In such a case, we would talk about the most famous AI tool being the neural networks. That sort of advancements would show some capacities to get used for machine learning, pattern recognition and control engineering as well as some cybersecurity purposes. The quite powerful weapon, you would agree with us?

From one perspective, the neural networks would so smartly mimic the human brain transferring the electrical signals through connections and using the activation functions in order to produce the activation potential. The majority of these instances would get tackled using the computing systems and those projects would increasingly need the skillful developers who would create the useful software solutions. The activation function would normally be some mathematical rule that would give us a chance to produce some signal. In other words, the neural networks' design and programming is definitely the job for mathematicians and you need to be seriously creative in order to make your own neural network. As we said – the neural networks got ability to learn and such an advantage could get applied in so many areas of the interest. For instance, if we talk about the cyber defense – we would notice that our neural network AI solutions could help us better understand the cyberspace and everything happening there. In addition, if we try to apply the neural network in cryptography, we could get the quite dynamic encryption that could offer us key, strong or even perfect ciphering. The opportunities coming with the neural networks and the entire AI wave are nearly limitless and if we attempt to correlate those areas with the quantum computing we could get so close to discover some secrets of the nature. As we know, the defense is about covering the uncovered details and if we try to apply something that fast learning as AI is – we could figure out what the weaknesses in our cyberspace are and how they could get repaired. The point is that the application of neural networks in cryptography could open us the doors to some new dimensions of science, technology and security at the same glance.

The future may seem so promising and hoping and if we take into account all the products of our technological revolutions – we would notice that the coming times could offer us so exciting landscapes. As we got so talented mathematic scientists to design the new and new generations of neural networks, we believe that the similar effort could get used in making the cryptographic systems being based on the AI. Such a sort of discovery could find the strong applications in a constantly changing environment as the web is. The human intelligence would describe the ability to cope with the unknown surrounding and if we try to observe the AI from such a perspective – we would realize why it's so important to get capable to handle any technological environment including the good defense solutions.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide

About The Author



Milica D. Djekic is an Independent Researcher from Subotica, Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the book "The Internet of Things: Concept, Applications and Security" being published in 2017 with the Lambert Academic Publishing. Milica is also a speaker with the Bright TALK expert's channel and Cyber Security Summit Europe being held in 2016 as well as Cyber Central Summit 2019 being one of the most exclusive cyber defense events in Europe. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2019. Her fields of interests are cyber defense, technology and business. Milica is a person with disability.

Copyright © 2019, Cyber Defense Magazine, All rights reserved worldwide