UNIVERSITY OF TARTU
Institute of Computer Science
Cyber Security Curriculum

Valeriia Avramenko

Cost-Benefit Analysis of a Hybrid Terrorist Attack on a Power Plant

Master's Thesis (30 ECTS)

Supervisors:

Hayretdin Bahşi

Raimundas Matulevičius

Tartu 2018

Cost-Benefit Analysis of a Hybrid Terrorist Attack on a Power Plant

Abstract:

In our thesis we want to compare costs between two different approaches that have the same goal – compromise a power plant by creating a physical effect (whether destruction of the whole facility or some of its parts and by that disrupting the power supply operation for a long term, optionally causing human casualties). We saw that in most research papers and media publications main focus is on just hacking into the power plant stating that it is way too expensive to become a usual practice for terrorists, unless state funded. We point out that physical aspect is often omitted – both when designing security systems of a facility and also when thinking about attack vectors and foreseeing threats to our way of living. Our main message is to think cyber and physical together – map logical topology to physical and see if some critical parts are easier to access physically than via logical cyber hubs. For modelling attack scenarios we use attack tree diagrams and for analysing resources needed to achieve stated goal we use cost-benefit analysis (with the only difference – benefit is the same for both cyber and hybrid scenarios). Our main hypothesis states that hybrid approach, combination of cyber and physical means to compromise the power plant, is cheaper than pure cyber.

This thesis is written in English and is 46 pages long, including 9 chapters, 12 figures and 1 table.

Keywords:

SCADA, Cyber Terrorism, Attack Tree, Cost-Benefit Analysis, Hybrid Attack, Power Plant, Critical Infrastructure

CERCS: P170 (Computer science, numerical analysis, systems, control)

Elektrijaamadele suunatud hübriid terrorirünnaku kulude-tulude analüüs

Lühikokkuvõte:

Uurimustöö sihiks on võrrelda kahe erineva, ühtse eesmärgiga lähenemisviisi maksumust. Mõlema lähenemisviisi eesmärgiks on elektrijaama ohtu seadmine tegeliku kahju tekitamise teel (s.h terve rajatise hävitamine või rajatise osade hävitamine, takistamaks pikaajalist energia tootmist, valikuliselt inimohvritega). Tuvastasime, et enamuses uurimustöödes ja meediaväljaannetes on peamine rõhuasetus üksnes elektrijaama häkkimisel, järeldades, et selline meetod ei saa kulukuse tõttu muutuda terroristide tavapäraseks tegutsemisviisiks (v.a juhtudel, kus antud tegevus on riigi poolt rahastatud). Osutame välja, et rünnaku füüsiline külg on sageli välja jäetud - seda nii rajatiste turvasüsteemide disainis kui ka ründevektorite analüüsis ja meie eluviisi ohustavate aspektide ennustamises. Meie peamiseks sõnumiks on analüüsida küber- ja füüsilisi osi kombineeritult - kaardistades võrgutopoloogia füüsilisele ja analüüsides, kas kriitilistele osadele on lihtsam ligi pääseda füüsiliselt või võrguühenduse kaudu. Rünnakustsenaariumide modelleerimiseks kasutame ründepuudiagramme ja vaja minevate vahendite uurimiseks rakendame tasuvuse ja kasu analüüsi (ainsaks erinevuseks on, et kasu on sama küber- ja hübriidstsenaariumide puhul). Meie peamiseks hüpoteesiks on, et hübriidne lähenemisviis - kombineerides küber- ja füüsilised vahendid elektrijaama ohtu seadmiseks - on odavam kui puhtalt küberrünnak.

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 46 leheküljel, 9 peatükki, 12 joonist, 1 tabel.

Võtmesõnad:

SCADA, küberterrorism, ründepuu, kulude-tulude analüüs, hübriid rünnak, elektrijaam, kriitiline infrastruktuur

CERCS: P170 **(**Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimis-teooria))

Table of Contents

1. Introduction

1.1. Aim of the Research

"What we're trying to do is introduce a culture where you expect the attacks and build in resilience so that when they come it doesn't really have much effect".

Dr Patricia Lewis, Research Director at Chatham House

The main goal of this study is to make a reasonable evaluation of how expensive and real it is for a non-state funded terrorist organisation to apply a combination of physical and cyber approach when trying to compromise a power plant. It is important to understand the first and foremost goal for terrorists is to cause fear. Which could be achieved by the striking result of the attack (such as physical destruction, people's death at best) and good media coverage. There are definitely no worries about the media – even not so harmful attacks on an object of critical infrastructure were present – so our guess is that if attack is heavy enough to cause death and/or physical destructions, it for sure will appear in the late evening breaking news section. Therefore we focus our attention on physical destruction aspect. We do not emphasise that much on possible deadly outcomes as it is something hard to predict and to work with; our final achievement is causing physical effect in one of the critical parts of a theoretical power plant.

1.2. Research relevance and novelty

As a cybersecurity expert Robert M. Lee, CEO of industrial cybersecurity firm Dragos, Inc., noted in his interview with "Scientific American", attacks against critical infrastructure become more and more aggressive [29]. After STUXNET the speed and he scope are only increasing. Attacks on Ukrainian power grids in Decembers 2015–2016, that left the whole region without power for hours [28]. "BlackEnergy" and "BlackEnergy2" (also found in the attack on US power grids in 2016 in Vermont [34]), malware targeting specific high level systems [30]. "Havex", crafted for industrial objects and so on [31].

It is arguable that the information-technology part is still relatively expensive [2], but we see that the toolbox is growing and there is less and less to tailor yourself. In addition to it we have time proof physical means of intrusion and destruction – relatively cheap, easy to comprehend. That is boosted with even higher demand on this type of attack and its influence. As a result we get a dangerous brewing that threatens to explode any day.

Maybe even right now there is someone planning an attack on industrial object, as we speak. So we might as well start getting prepared.

Also we rarely see people thinking about cyber and physical together. If they look at the network topology, it gives them information on how many hubs should be passed to get to the target. But what if by looking at the physical locations of those server it is easier to get through one hub which would allow the attacker to compromise the next one by physical means by just being there? That is why when we protect our network we should also keep the physical protection relevant to the object's importance.

Our contribution is looking in a new way at the critical infrastructure and power plants as such. We apply a mapping between physical zones and logical hubs of the network topol-

ogy to see what are the protective measures and point out if there are relevant or not depending on importance of those hubs and servers. We also band methodologies to suit our purpose – we want to compare costs involved in achieving the very same goal but in different ways – pure cyber scenario and the hybrid one (where we combine cyber and physical means to move forward). For that we use attack trees for building our scenarios and cost-benefit analysis to present evaluation of our nodes (keeping in mind that benefits are equal and we are comparing costs only).

1.3. Research Questions

This thesis makes its best to answer the following questions and concerns:

1. How much would a hybrid terrorist attack costs?
2. Is it even a plausible scenario that terrorist would choose when there are so many other options to cause death and fear?

1.4. Research Scope

To narrow down our field of research, we are mainly interested in intrusion techniques that the attackers might use. Other means, such as ransomware, encryption etc are not that important to us as they do not lead to a physical damage. We are looking into different access points and ways to infiltrate the system that would allow the attacker to get inside the power plant and cause an actual physical damage – whether to people inside or critical systems in the secured zones. Which means that we do not look exactly at the STUXNET scenario [6], where physical damage was caused, as it was done only by cyber means and nobody has died. STUXNET was a precedent, but it has lost its novelty over the time. We are looking into more actual type of a threat that can still surprise public.

We are also keeping our focus on the Stage II type of attacks – those that result in temporary loss of power, physical damage to equipment or other actually visible impact [29]. Though Stage I attack, performed mainly to obtain information, can be a stepping point for our end goal with the notation that it will be targeting information from a specific system to learn more about it so that a tailored exploit can be made and later activities would be more accurate for the object [33].

1.5. Agents

There are quite many actors that could consider such attack. Let us have a closer look at these groups and define our persons of interest. The most common types can include script-kiddiez/hobbyist, cyber criminals on someone's payroll, state sponsored groups etc. For the purpose of our research we focus on non-state funded terrorist organisations.

Script-kiddiez and hobbyists

By definition script-kiddiez do not have applicable knowledge nor resources to perform this kind of attack. Frankly, they also lack motivation to do so – too hard to achieve, too high responsibility level [12]. If we imagine a typical hobbyist, it is a person who explores the area, might have some intentions and able to find tools, written by others, to hit from

low to middle range of troubles [13]. Therefore getting hands dirty on a power plant is out of their competence. For now.

Hacktivists

The main difference between script-kiddiez and hacktivists is their motivation. The later usually have a political view to defend or to show their position regarding social matters. Hacktivists vary in their competence and they even make claims to be able to shut down the whole Internet [14], but so far no real damage was made. Also attacking a power plant might not be the most preferable vector of attack for them as it is a neutral object that usually does not represent any political party, group or a process. Therefore it is not a very plausible scenario to consider at the moment.

Cyber criminals

This type of attackers usually consider profit as their main motivation therefore taking down such a massive facility would only be by orders of a superior power. In which case it makes more sense to consider that power as the main actor, not criminals themselves as they would not be constrained with the financial part of the deal, they will be paid just enough to implement it.

Non-state funded terrorist organisations

We do not consider state actors by default as we assume that they have unlimited set of resources which makes any type of attack accessible from a financial point of view. Therefore **our main attacker is a non-state funded terrorist organisation** – which means any group of individuals that uses terror as a tool to achieve their goals, mainly political ones [15]. The list is quite long, the most known entities are ISIS (Daesh), Al Qaeda, Hezbollah etc. Some of them have already claimed or even planned an attack on a power plants but so far no success has been seen [16]. This general category of attackers shows the most motivation to attempt an attack on a power plant and also has much wider resources compared to other groups [28], which is why we chose it to be the main actor in our attack model.

1.6. Agent's Motivation

The main reason behind such attack is its scope. A power plant is a facility that provides resources to the whole communities and other services such as hospitals and somehow critical establishments. The scope is important as it maximises the amount of people affected and therefore their fear. One of other options would be to use some sort of a weapon of mass destruction, but those are difficult to get in a quiet manner, hard to sustain and also require much higher and more specific expertise [17]. Also power plants as a vital part of energy supply system have become symbols of Western World technology – something that most terrorist organisation claim to fight on a fundamental level. They portray West as a mechanism without a soul, without the right religion and without any right to claim itself as a developed civilisation. Therefore attacking a power plant caries very important symbolic message in itself.

Another reason for that is that long absence of a power resource can cause public unrest and even riots, that can be enough to destabilise a country and its government [24] [26].

This can be used in misbalancing political power distribution in a region with further follow up steps.

1.7. Research Limitations

"The sky's the limit. Your sky. Your limit".
Tom Hiddleston

One of the main limitations in constructing the attack tree is our imagination. It is nearly impossible to say if a certain attack tree is complete as there are always more options to achieve the same goal. There is basically endless set of possibilities to how the end goal can be reached – from an absolutely new path to a set of small differences in each node. Not to mention how subjective this approach is; two different people would come up with two very different attack trees even if given the same facility to attack and the same means to do so. Therefore the result of our research covers only some of the scenarios that could unravel in such setup. But to provide better image of possible attack vectors we looked at what has happened before, what was claimed, what was threatened and what ideas were applied to other objects.

Another constraint is how much our attack tree depends on initial parameters and what we know about the attacker, which is also limited by natural causes of not having enough information about certain terrorist groups capabilities. We can model, we can read through news articles and other research works, but we can only try to make it as close to reality as possible, it will never reflect the real situation fully.

We also provide prices for certain skills, materials, acts and devices as for today and this can change with time and so diminishing the relevance of our results. But to the fairness, we are trying to understand if such attack is plausible to be performed today, therefore our time borders are aligned with our results.

Last but not least, it's nearly impossible to model a universal attack tree that could be applied to any power plant without losing precision. Every facility has its own topology, internal rules and regulations. What is possible to perform in one place, would not get adversaries as far in another location. So our goal is to strike a balance – to cover scope wide enough to be representative of the results, yet save level of precision that would still be enough to show the point and to be relevant.

1.8. Thesis Structure

After stating definition and having a look at the literature review in chapters 1-4, we describe in Chapter 5 our methodology and how did we change canonic methods to suit our research purpose and reflect end results better.

After that we would have a couple of words in Chapter 6 about the background scenario that describes a prototype systems that our theoretical attack would want to compromise. We will describe its network topology, physical plan and how is it connected to each other.

In Chapter 7 we already present our designed attack scenarios in a shape of attack trees and clarify how does it all go along and what inspired each path and node. It directly leads to result calculations in Chapter 8 and is summarised by a conclusion in Chapter 9.

2. Terms and Notations

In order to ensure that everybody understands the thesis the same way, we clarify the main terms and notations used in our research.

Power plant (Estonian *elektrijaam*) is a complex of structures, machinery, and associated equipment for generating electricity from another source of energy, such as nuclear reactions or a hydroelectric dam. Also called generating station, power station [1]. Power plants are part of the critical infrastructure as they produce vital energy to a big scale of customers. It provides electricity to the end users such as other infrastructure objects, cities, villages, business structures, households and others.

Hybrid terrorist attack (Estonian *hybrid terrorirünnak*) is an attack performed by established terrorist organisation which uses both physical (explosion, intrusion, destruction etc) and cyber (remote access, video surveillance control, machine infecting) means. As a cyber part we include but do not limit to:

- direct misuse of cyberspace facilities that are connected to the target;
- intrusion in a computer network or system;
- espionage in a sense of collecting information from a target's systems and databases..

SCADA systems (Estonian *SCADA süsteemid*) stands for "Supervisory Controls and Data Acquisition" and is a set communications protocols designed for the exchange of control messages on industrial networks" [20]. So we are talking about the system that takes care of our power plant maintenance and internal communications, along with ensuring that facility is secured. There are many specific protocols for different types of the critical infrastructure objects – MODBUS, DNP3, EtherNET/IP, PROFIBUS, Foundation Fieldbus etc – each tailored to serve specific purposes and types of communication.

So far efficiency of passing on communication was more prioritised than security. At most, security concerns were covered by isolating the whole system from the outside world and networks. But as automation and global integrity rise, it is no longer a case – you can see plenty of power plants and other objects of critical infrastructure connected to the Internet [27]. As [power] grid cybersecurity expert Robert M. Lee, CEO of industrial cybersecurity firm Dragos, Inc. pointed out, "...because of business reasons, because of lack of people to man the jobs, we're starting to see more and more computer-based systems. We're starting to see more common operating platforms. And this facilitates a scale for adversaries that they couldn't previously get" [29].

If you even just search for "SCADA" at https://www.shodan.io/, it will show you at least 600 connected systems [22]. We can see what SCADA protocols they use, what SSL version and even the operating systems they use as the hosts! There we can also check the "Exploits" tab to see how many different exploits were already created and reported, straight to their source code [23]. Therefore, we can see that this set of protocols is highly exploitable and targeted.

This is mainly due to the fact that "...most SCADA protocols were designed long before network security perceived to be a problem. The traditional SCADA system was a closed serial network that contained only trusted devices with little or no connection to the outside world" [20], which means that we put part of our critical infrastructure security on legacy.

3. Problem Statement

"A problem well-stated is a problem half-solved".
Charles Kettering, inventor

Even though the studies in the literature do take a terrorist threat as a major point in general assessment, it still concentrates mostly on pure types – totally physical or full cyber attack. To the present time they analyse a terrorist organisation capabilities from the point of view of how many bombs can they produce and how close can they come near the target. Usually they dismiss the possibility of a pure cyber terrorist attack (not a state funded) in a nearest future by reasoning it with a high price and complexity of such action. "The [terrorist attack] planners would conclude that costs are high, outcomes are too uncertain for an untested practice such as this and, ultimately, few Internet attacks would directly kill people. They would suggest that, for the time being, the organisation should concentrate on more traditional core-business (for instance, car-bombs), while waiting for three conditions to occur" [2] (low price, certain results and direct casualties).

In her study Maura Conway also advocates the small likelihood of pure cyber attack by referring to the main goal of a terrorist action – spread fear. "Because 'real world' [physical] attacks are cheaper and less complex while also being significantly destructive of lives and property and, importantly, emotionally impactful so therefore also attention-getting to an extent that cyberterrorism will struggle to achieve" [3]. If people don't see a fire, it's hard to make them feel scared and start panicking.

Our goal and contribution is to test this believe allowing an alternative scenario to unravel – a hybrid attack, which combines cyber and physical parts, hence lowers the cost of the whole agenda and thus making it more attractive for the terrorists to implement. We will look at the situation that answers the question "What if terrorists use cyber as a supportive tool, and mix it with the usual physical actions?". This hybrid approach gives terrorists so much more possibilities and attack vectors – if with just a suicide bomb they can damage the surface, then with disabling video surveillance they can come much closer and create even bigger damage.

As a result, we want to test the following main hypothesis (smaller clarification could be formulated during the research):

H0: Hybrid attack is significantly cheaper compared to a pure cyber attack for achieving the result that is equal in damage.

As a target was chosen a power plant, but this principle applies to any Critical Infrastructure Object (CIO). Choosing a concrete kind of CIO allows us to build a prototype system for a better demonstration and analysis.

4. Literature Review

Bangs for the Buck - A Cost Benefit Analysis of Cyberterrorism by Giampiero Giacomello

This article is mostly role-plays from a perspective of a hypothetical terrorist group (not a state sponsored), which might get interested in applying cyberterrorism in their toolkit. To summarise it, we can just quote the study itself: "This article argues that, under these conditions, cyberterrorism would be a highly inefficient solution for terrorists, due to high costs and meager returns. The article explores these questions and hypotheses by applying the economic efficiency logic of cost-benefit analysis" [2]. By "these conditions" author means that the initial goal – *break things kill people* – is much easier achieved by following traditional means as making bombs, taking hostages etc – it is cheaper, more spectacular and calls for an attention of the general public, not only technical specialists who could be concerned about a cyber attack.

From a positive side, "Bangs for the Buck…" gives a very wide analysis on a matter of cyberterrorism and what is its practical usage. We can derive both quantitative as well as qualitative analysis on a given data. It also states strict and clear conclusion that cyberterrorism is not something we should be afraid of in the nearest future (5-15 years).

The downside of this study, but could also be intentional, is that Prof Giacomello looks at a very pure type such as cyberterrorism. He analyses only those attacks and threats caused purely by cyber means. And what we see from a current state and news – that is not what is evolving right now. There is no jump between technologies – they are applied in a more gradient way, step by step. So if we take author's words "that is not going to happen in the next years" we might find ourselves in situation when it is way too late be concerned by something which is a reality already.

Hybrid: what's in a name? by Jan Joel Andersson and Thierry Tardy

The article in its essence tries to narrow down terminology of a hybrid warfare – which includes both physical and cyber means, along with conventional and non-conventional ways of attacking. Authors present their view on hybrid threats in these words: "Simply put, for a threat to be of a 'hybrid' nature it needs to be the product of multiple ways to threaten or attack its intended target – much as a hybrid species is produced by combining different breeds or varieties. It is therefore the mix of different methods – conventional and unconventional, military and non-military – which makes a threat hybrid" [5].

The article argues though that just by using cyber means the attack cannot be presumed hybrid by default – it also depends on its aims and more of intermediate aims of using technologies, as said: "Terrorism, cybercrime, trafficking and extortion are not per se hybrid in nature; they may become so depending on how (and to what extent) they are pursued using multiple tactics simultaneously" [5].

It is a relief to see somebody to actually attempt to see combination of cyber and physical means and even put it in the common structure. Though in this article, even though it tries to clarify things, it might just confuse them even more. Authors do not state clearly to what category should combined approach belong, as well as they put way too many differ-

ent things under one hood – such as naming both combinations of military/non-military and physical/cyber as a hybrid type of an attack.

One of the crucial points here is that with certain type of attack the corresponding response is required. On example of a non-military attack authors explain that a non-military approach should be applied. Which also projects itself of our focus – if we expect terrorists to use both physical and cyber means at the same time, we need to build our defence systems accordingly.

Cyberterrorism After Stuxnet by Thomas M. Chen

This work analyses our view on the world after Stuxnet events started in 2010. It mostly focuses on one and only precedent of cyber attack which is known to cause a real touchable impact. Before Stuxnet "…terrorists are known to be using the Internet for various routine purposes. The discovery of Stuxnet in 2010 was a milestone in the arena of cybersecurity because, although a malware attack on industrial control systems was long believed to be theoretically possible, it was different to see malware used in reality to cause real physical damage" [6].

Even though here we see an actual cyber attack present, the general view remains sceptical about future possibilities. Stuxnet was exceptional and it stays this way – an exception. Thomas Chen says that from a cost-benefit point of view balance did not change, and Stuxnet malware is not reusable as it was very well tailored for that exact set of infrastructure so redoing it for a more unified usage would be the same as writing a new malware from a scratch.

We can see that again focusing on a pure types of attack do not give us much of a perspective as it goes far from a real world situation where combinations are shown to have much higher level of efficiency and convenience.

Reality Check: Assessing the (Un)Likelihood of Cyberterrorism by Maura Conway

Dr Conway in her research looks at the likelihood of cyberterrorism from a perspective of four hypotheses:

1. "First, the costs of cyber attacks – although difficult to estimate – are vastly higher than those of non-cyber equivalents, such as car bombings.
2. Second, terrorist groups typically lack the mastery to carry out successful cyber attacks which are exponentially more difficult than non-cyber terrorism.
3. Third, the destructive potential of non-cyber attacks can be far more readily materialised than that of cyber attacks.
4. And, fourth, cyberterrorism lacks the theatricality of more conventional attacks and therefore is likely to be less desirable to terrorist groups" [3].

The conclusion would be the same as other authors came across, but Dr Conway goes a bit more realistic and states that we do not actually know about capabilities of terrorist groups. We can only judge by what did they do already and we have no access to what they might do in any observant future. There is no bulletproof intelligence and any data can be questioned.

But still comparing cost of a pure physical and pure cyber attacks author sums up that for now physical means are cheaper and much more visual than cyber is going to be in any observant future. She compares Stuxnet with Boston Marathon bombings, where just low home-cooked bombs caused several deaths and huge media attention along with the public response, whereas Stuxnet is still not widely known and not so many people can even comprehend what exactly has happened there. Both bombs and strategy applied were of a very low quality, but Stuxnet by approximate calculations might have cost more than 10 millions US dollars [3]. So far so good, seems like an obvious choice.

Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games? by Michael Stohl

Here article actually points to a very crucial moment – where is the line when we can call an attack to contain "cyber" in it in any way? It states that in general there is a failure in distinction between using Internet and other technologies for organisational purposes such as communication and information transfer and using digital part to actually commit an attack. Therefore it calls for a clear understanding what is a cyber part of an attack.

This article shows that cyber side of terrorism was a valid concern 10 years ago already. "Much before 9/11 there had been great angst about the possibilities of cyber terrorism, including oft stated fears about a digital Pearl Harbour. This fear was further enhanced by the Y2K problem often referred to as the millennium bug by those who sought to dramatise the threat. Despite the fact that these fears have yet to be matched by real events, in the context of the post 9/11 concern with terrorism and the global war on terrorism, the threat of cyber terrorism remains high on the list of public and professional fears" [7].

Though this source is much older than other looked at in this review, the author already takes into account possibility of a mixed approach. He mentioned that in old times Al Qaeda group was learning how to fly, now there are acquiring a new skill – hacking. And as we see nowadays, they are doing quite well.

Quite realistic and sane view was presented by Dorothy Denning, when she was speaking to the Special Oversight Panel on Terrorism of the Committee on Armed Services of the U.S. House of Representatives, mentioned in this article: "Thus, at this time, cyber terrorism does not seem to pose an imminent threat. This could change. For a terrorist, it would have some advantages over physical methods. It could be conducted remotely and anonymously, and it would not require the handling of explosives or a suicide mission. It would likely garner extensive media coverage, as journalists and the public alike are fascinated by practically any kind of computer attack. Indeed cyber terrorism could be immensely appealing precisely because of the tremendous attention given to it by the government and media" [7].

Among other things this work actually has shown reasons why cyber means might be attractive for terrorists groups. They allow to cover activities, safe resources such as lives of group members so recruiting would not be such a bargain etc.

4.1. Aurora Generator Test

As a separate point we would like to analyse an example of a physical impact of a cyber attack. Such demonstration was performed in 2007 by Idaho National Laboratory and is

known as Aurora Generator Test which involved controlled hacking into a replica of a power plant's control system [32]. In a nutshell, by having a remote control researches were able to rapidly open and close a diesel generator circuit breakers out of phase from the rest of the grid and cause it to explode.

"What people had assumed in the past is the worst thing you can do is shut things down. And that's not necessarily the case. A lot of times the worst thing you can do, for example, is open a valve – have bad things spew out of a valve," said Joe Weiss of Applied Control Solutions [32].

From the video footage of the impact in the controlled environment we see that the attack was able to take the equipment out of order completely and rather fast[1]. If we apply the same result to a system of a bigger scale, it can lead to months before power can be restored. Hardware is the hardest part to fix, as we also saw in Ukrainian attack – several operations are still performed in a manual manner because of hardware damage [29].

From a price perspective potential impact is described as:

"For about $5 million and between three to five years of preparation, an organisation, whether it be transnational terrorist groups or nation states, could mount a strategic attack against the United States," said O. Sami Saydjari of the nonprofit Professionals for Cyber Defense. Economist Scott Borg, who produces security-related data for the federal government, projects that if a third of the country lost power for three months, the economic price tag would be $700 billion. "It's equivalent to 40 to 50 large hurricanes striking all at once. It's greater economic damage than any modern economy ever suffered. It's greater than the Great Depression. It's greater than the damage we did with strategic bombing on Germany in World War II" [32].

But we need to keep in mind that here they are assuming full cyber attack that does not involve any physical additions to complement the main process. Also these calculations were made in 2007 which means that with advancing technology many parts became much more cheap compared to then.

[1] https://youtu.be/fJyWngDco3g

5. Research Methodology

In our research we combine two methods, where one helps to provide a comprehensive model to describe scenarios and other gives a simple and rather certain way to evaluate those scenarios in a context of their cost.

5.1. Attack Trees for Modelling the Scenarios

One of the biggest challenges in cost assessment is to separate intuition from numbers based on facts. Our intuition takes into account only our overall experience and sometimes irrelevant memories which could easily lead us to making wrong decisions. Also intuition is not much of a help in new, unknown conditions. To overcome this constraint and have a better overview of the situation multiple techniques were developed.

To present the model of our attack scenarios that we compare we use Attack Tree type of diagrams. It gives structured and focused overview of the situation we describe in a compact and easy way to comprehend. It also allows us to have some space for variations and flexibility, as well as the help our imagination to picture the link between actions and their consequences along with the effort and preparation step that take us to the main goal by saving the logic of certain attack as the relation *"father –> son"* between nodes.

We will construct a prototype system to which these attack trees apply. We would need two trees – one for full cyber scenario and one for hybrid.

"Attack trees are models of reality" [4] – they show different paths that could be taken to achieve the ultimate goal – the root node. Our ultimate goal we define here as creation of physical damage. It reasons by the fact that any terrorist attack pursues the BTKP – *break things kill people* – type of impact.

Attack tree in its essence is a decision making model that demonstrates different ways of situation progress and its consequences. It is widely used in security risk assessment and attack modelling as it allows to predict attacker's behaviour in the most precise way – because the main focus here is on the attacker, his actions are being described and analysed, not the defender capabilities. In this type of analysis we are trying to see what could be done to us, rather than analysing from what kind of attacks we are able to protect our system. If we look at the threat model from this point of view, it decreases the possibility of missing something or overlooking certain action for which we might not yet be prepared. In attack tree construction defender's abilities are not taken that much into account, it is purely a description of attackers capabilities and paths he might take, along with the decisions made and tools used. Defence mechanisms can only be a part of reasoning for levels of sophistication and increased cost because the better system is protected, the more expensive and hard will it be to penetrate.

Potential attack tree would be applied to a hypothetical structure of the power plant, simplified for the sake of a better overview and modelling. Here we would concentrate our attention on physical access levels which can vary from general area to critical closed objects.

Access zones of our power plant are defined as:

1 – critical area, restricted access, biometric authentication;

2 – administrative area, restricted access using assigned card and/or passwords;

3 – general area, access is somehow restricted to only workers of the object and verified visitors.

We can assume that all zones are covered by video surveillance and there is no "white" zones. We cannot guarantee any level of loyalty to the facility of the working personal as we use the insider scenario as a possible assumption to support some of our attack vectors.

It is very important to define both attacker and defender for a particular attack tree as it influences its scale and variations hugely. A good explanation for this need is provided by Terrance R Ingoldsby:

"Attack tree analysis incorporates information about a specific defender's adversaries and the benefits they will realise from carrying out an attack against a particular defender. This precision is a virtue because it offers the hope that predictions will be accurate for a given situation. However, this specificity also makes it difficult to compare defender-specific predictions with statistics that are generalised over a wide variety of defenders and attackers. For example, consider two technically identical security systems. The risks associated with a particular attack may differ considerably between the systems because the assets they are protecting also differ. The different potential rewards may attract different adversaries with different skills, resources and motivations. Technically identical failures can have significantly different business impacts on their respective organisations (which also affects the risk)" [4].

Also one of the challenges that goes along with the attack tree is working with unknown. Most of the assessment tools base their evaluation on statistics data and events that occurred before. Attack tree, from the other hand, also has in its structure threats that have never been performed before. Proposed methodology leaves it fully to the scale of fantasy of the researched who has to come up with the ideas about all potential dangers. When constructing the attack tree, we need to take into account both past events along with the feasible combination of tools and intentions that could produce totally new result.

We can somehow compare attack trees with decision making trees that are applied in business and financial planning. With the only difference – here we would need to play a role of an attacker and then tree will represent adversary's decision making process with its paths and options.

Downside of attack tree is its dependency on strict parameters. To build a feasible attack tree we have to know our attacker and his capabilities quite well. We should be aware of his skills, physical and cyber capabilities, it is also very important to know and understand his motivation which would give us a hint on how far he is willing to go and how much to sacrifice only to be able to cause the root event. Attack trees also rely on our ability to think as an attacker and go out of usual frame of events. We have to be able to come up with new ideas of what could happen because that is exactly what attackers do – there are some time-proof methods and actions that they use more or less on a regular basis, but their aim is to come up with new ways of destruction and spreading fear. Both sides evolve, so both sides have to adjust and be creative.

Attack tree gives us a good set of data to then create a secure and less vulnerable framework, but it requires a lot of our imagination and role playing to collect the initial data for us to analyse.

To verify results and do an error assessment we use references for each node that describes the scenario we are presenting and gives information about the resources required to get to that node and perform stated action.

Attack trees allow us to plan our security measures taking possible threats as a background, our foundation. We go step by step on every more or less real action that could be performed against our system and evaluate its probability. As a final result attack tree gives us a clear idea of possible attack vectors in one big pictures filled both with context and comparable options.

5.2. Cost-Benefit Analysis for Evaluation

As for the evaluation and comparison between two scenarios – a pure cyber and a hybrid one – we use cost-benefit analysis that would give us a clear answer to which way can be more preferable and affordable for groups and associations that we present as our attackers, namely non-state funded terrorist organisations. By its definition, "Cost benefit analysis (CBA), sometimes called benefit costs analysis (BCA), is a systematic approach to estimating the strengths and weaknesses of alternatives (for example in transactions, activities, functional business requirements or projects investments); it is used to determine options that provide the best approach to achieve benefits while preserving savings" [18]. Basically, it allows us to see the total sum of resources spent on achieving a concrete result and be able to compare those sums between themselves. By resources here we mean amount of money required to cover the cost of each attack scenario.

In case of our cyber component, we can evaluate how much money does the equipment cost and what is the market price for the skills needed to cover those nodes.

One of the advantages of using CBA analysis is being able to analyse data that is closely tied to reality – we do not just fantasise, we also verify how close our ideas are to the real world. It also gives us simplicity as the idea behind this method is to see whether benefits outweigh cost and make our decision based on that. From the other side, it also requires us to be as precise and accurate with our resource estimation as possible. CBA gives us an easy way to present our calculations, but if source data our our assumption is wrong, the final result will be far from a plausible representation of researched scenario [19].

Our final goal is to determine how much a certain scenario would cost in a sense of money and other resources (equipment and intellectual level, but mainly we are talking about money). This will allow other researchers in the future to use this result to reason if terrorist organisation have enough money to conduct such attack if someone would ever start a research on a potential terrorist organisation budget.

For simplification and better comprehension we will build a prototype of a theoretical model of a power plant, including its network topology and physical infrastructure, as well as map them together.

We will validate our results by providing relevant reference for each node, action and price we find.

5.3. Cost Function

In our research we define benefit as achieving the main goal, root node of our attack tree, and cost – as the amount of resources required to get to that node. Which means that benefit is the same for cyber and hybrid scenario – a physical destruction. Therefore we only compare costs as it can require different amount of resources to achieve the same goal. So we modify the method a bit as we will not compare benefit to cost (as benefits here are the same), but rather cost of different presented scenarios to see if our assumption of hybrid to be the cheapest one is correct. Therefore as a **cost function** for the path we will use the following logic – cost of the root node consists of costs of its children. If those have OR relation between them, then the cheapest cost is added to the cost of the parent; if AND – both costs are added. In this case the total sum for the end goal will be determined by the cheapest path and we just need to see which one will it be – cyber or hybrid (bids on hybrid).

If some leaves are repetitive, to avoid computation doubles we count the cost of repetitive path only once and omit it for other nodes focusing on the total sum instead of being precise about each subgoal. So if for retrieving the personnel data and for compromising the badge scan it is required to research the system that involves some costs and both of those subgoals are required to achieve the root goal, we will only count cost of researching the system once.

In some cases the node will purely consist of cost of its children, sometimes it will have additional resources added for that specific action as attackers might need additional resources to fulfil a particular sub-goal. Here is an example of how it works for our research:

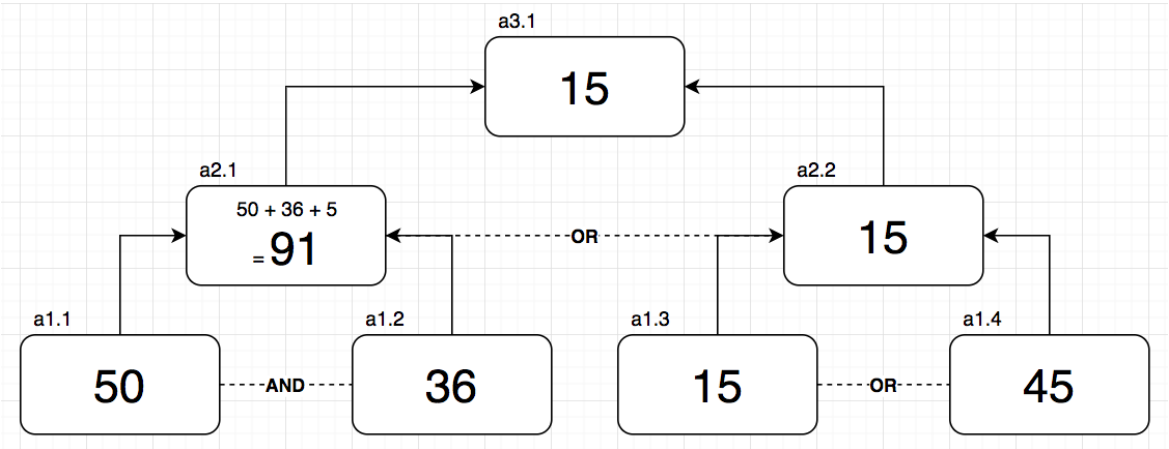

Figure 1. Cost function

We defined prices for the starting leaves a1.1, a1.2, a1.3 and a1.4 – these would be taken from reference articles and other resources. Next level is partially defined by the lower one with some additional costs involved – we can see that a2.1 has in it costs of its two children (given that they have AND relation) and also has +5 cost units to itself (as if this node requires extra cost units to be completed in addition to children's cost). The a2.2 node has children with OR relation and has no additional cost involved – so we take the cost of the cheapest child. In the end our root note has OR relation between its own children so we again take the cheapest one which results in the total cost of 15.

6. Background Scenario

In this section we are going to present the general physical settlement of our target – a power plant – and the exact goal that we want to achieve when executing scenarios shown in our attack trees. We will not go into much of details like length of security code or anything like that, because our mission here is to give basic overview of what might go wrong and in what scenario so later we can create our defence strategy based on that.

First part will describe the physical infrastructure of a typical power plant, including access levels, usual means of security and perimeter plan. In second part we discuss more what we want to achieve from a perspective of a non-state sponsored terrorist group and their motivation to do so. And finally in third we will try to make a connection between first two and show what that group can do in on given playground and try to predict some consequences.

Practically we can divide our target in three perimeters – **"owner-controlled area"**, which corresponds to the lowest level of security and can even be a part of a "guest area" still with with somehow controlled access (scan gates for example, to ensure that no restricted materials or items are brought into the facility); **"protected area"** is already secured with badge scan and more sophisticated security means – this area can have some control centres and SCADA servers, laboratories etc; and finally – "**vital area"** – which is the innermost circle, as far as possible from "owner-controlled area" and has in place the highest level of security and the most sophisticated defence means. The "vital area" is usually the reactor, cooling mechanism, used fuel rooms, alarm station, parts of SCADA systems, and other life-dependant facilities [8]. In general we would certainly like to isolate vital area from outer access, which means that this area is not connected to the Internet. Also security measures are designed to include safe shutdown of the system in case of a breach (we keep in mind that nothing is absolutely unbreakable).

Though we can already assume that disconnection from the Internet still cannot save the system from the breach. As the situation with Stuxnet attack on Iranian nuclear power plants has shown even fully isolated environment can hold a cyber attack. So for that our prototyped power plant also has a CERT team in facility that is supposed to deal with the accident caused by an attack if such is to happen.

Means of physical access control may include but not be limited to:

- "physical barriers, electronic detection and assessment systems, and illuminated detection zones;
- electronic surveillance and physical patrols of the plant perimeter and interior structures;
- bullet-resisting, protected positions throughout the plant;
- robust barriers to critical areas;
- background checks and access control for employees" [8].

This typical set gives a general overview of what kind of attack it is trying to preserve from – physical intervention, attempt to use unauthorised ID, insider man. For the attacker it is very important to also understand defenders mind so the attackers will not waste energy and resources to act in a way that is already taken into account and put as an orientation for a security system. It is always a mind guess and who is lucky to get it first.

In our scenario we put the main focus on surveillance and physical access points such as scan gates and badge authentication at doors between different zones.

In this sense seems reasonable to move to our second part – what do we want to do with this power plant? How do we want to disrupt its workflow and why would we want to do this. The possibility of a terrorist attack on a power plant or any object of critical infrastructure is a media background noise for quite some time already. From *"Diehard 4"* to already performed attempts of various sophistication such as sniper attack on California power station in April 2013 [9] and others. The recent report from Chatham House alerted that UK power plants are awfully unprepared for a cyber or mixed type of attack [10]. The main issue raised there was reliance on commercial software suits and utilisation age of some facilities – basically most of UK power plants are not even designed with current attack scope in mind, and we are talking here about one of the most advanced nations in a sense of security and intelligence. We can assume that countries with deeper history of neglecting outside threats might have even bigger gaps in their infrastructure design.

Our goal, and basis for the forthcoming attack tree, would be an assumption that terrorists' goal is creating physical damage and system disruption in the "vital area". There were already mentioned a few incidents with the first two access levels, but we know that the ultimate goal is always to go further and cause as much and as critical damage as possible. In this sense successful attack on the vital area is an absolute win for our prototyped group!

A few words about the group itself, so we have a basic understanding of the who we are dealing with. This group is a not state sponsored so they have somehow limited financial support and resources. They have access to the basic trainings for both physical attacks – bombs making, fighting, shooting etc – and knowledge base for cyber intervention. They have their motivation which can vary from political to religious or semi-personal even, they believe that workflow disruption will be a justified act to draw attention, scare, punish or whatever else is the main move here. They want to *break thing and kill people*, spread fear and call for action. They do not take into account their own lives – dying but still performing a successful intervention would be a win for them.

Drawing the line, this group's main goal is to damage the prototyped power plant enough to cause its shutdown, ideally distortion, and if possible cause some effect on human lives who might be working there on be dependant on functionality of this power plant.

With a described decorations and leading actors we can now start building up our scenario. For attack to succeed a few moments should be accomplished:

1. **get-in:** our group should be able to get in the system without being noticed or tracked, they should gain access to all areas including vital and have enough time to be there insensibly;
2. **plug-in:** they should be able to place the destruction mechanism (bomb, electric impulse generator, bonfire, anything) as close to the reactor as possible to cause the maximum damage;
3. **win:** even if they get there and place the "bomb", they still need to make sure that it works – this should mean that defence mechanism on the place would not be able to contain the explosion (stop it from affecting systems and spreading) and nothing else

will prevent the attack group from finishing the operation (such as security personal that can appear at the site and stop the attackers);

4. **(optional) get-out:** if attackers manage to escape from facility after performing an attack, it means that our system fails in reaction phase – even if attackers got in, security measures would prevent them from escaping so they can be called to responsibility and applicable punishment and payback.

Preparation steps would include:

- collection of information about the inside structure and scheme plan of the facility, its security means (time intervals between checks, locations of the guards, surveillance centre etc);
- applicable trainings for both physical and cyber so destruction mechanism could be created and security posts passed;
- planning the post-attack action which might include escaping the perimeter or even just making sure that media got the image and aftermath is directed by the remaining members of the group so it will not be for nothing.

With this basic build up we can already start our journey into attacker's mind and try to foresee how, where and what can go wrong. Now let us learn in more details how each security area is defined and protected.

6.1. Network Topology and Access Levels

As an orientation and example for our research we will use a sample topology from Yocogawa Whitepaper Plant Network Security [11] given below:

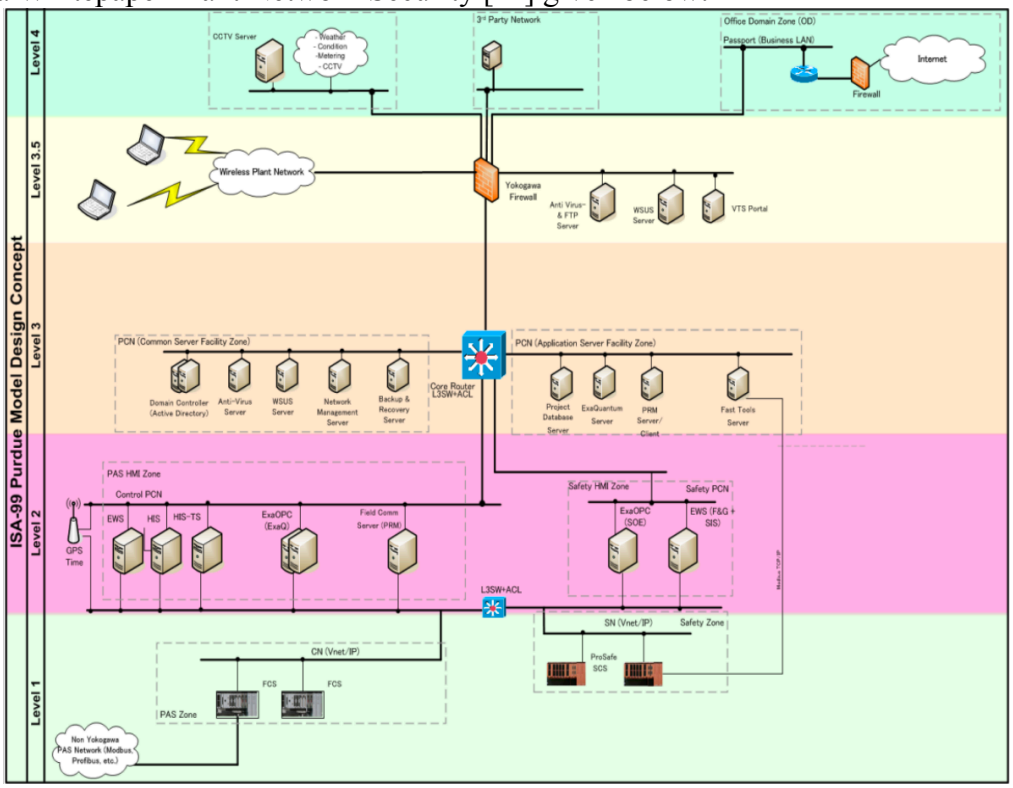

Figure 2. Network topology mapped to physical levels

Level 4: Owner-controlled (general) area

Outer perimeter, sufficiently distant from the main vital area, minimal level of security including video surveillance, package control scan (alcohol, explosives, firearms are prohibited). Network part includes “office zone” that is connected to the outer world (Internet), but is protected by firewall and some anti-virus scanning systems. The 3rd party network can be another department in its own VLAN. We can see that CCTV server that are responsible for the video surveillance of the whole facility are also located in general area, which makes it easier to compromise and use or shadow to go further. Here are also located servers for badge scan match to access the protected area (levels 3 and 3.5).

Level 3 and 3.5: Protected area 1

Includes administrative end-devices and VTS Portal servers. Behind the firewall, but in the same physical zone, we also see WSUS (Windows Server Update Services) server, that is responsible for distributing software updates around the facility. Which means that having compromised the access point between general and protected areas gives us admin access to pretty much the whole network and allows attackers to install whatever software needed that would look like an update – would not be the first time for Windows [36].

Level 2: Protected area 2

It is the location of the Safety PCN – Process Control Network, that is a communications network that is used to transmit instructions and data between control and measurement units and some parts of SCADA equipment. It also has servers for the biometric scan databases that verify access to the vital area.

Level 1: Vital area

From a network perspective this zone locates some of the SCADA servers and control networks. Apart from that it is also where the main reactor, cooling systems and direct control panels are placed. This is the main point of interest, finish line for our attackers. Getting here means winning the whole thing.

7. Attack Trees

"A chain is only as strong as its weakest link"
Thomas Reid

When building an attack tree and assigning a corresponding value to each node, we need to keep in mind the level of available tools for each task to be performed. It is also important to mention that this can change with time and some task will require less resources as more tools and knowledge will become freely available for use [25]. Therefore our results are to be taken in the context of a current timeframe – 2018 and around 5 years after.

As our root goal we take a physical impact. Just hacking the power plant is not in our scope of interest anymore, something should be explicitly broken – service disrupted for a longer time or some part of the power plan destroyed – as the result of this attack. Possibly the whole facility goes out of order and maybe some people get injured. Intention to cause a visible consequence was already expressed therefore we need to focus our attack scenario on BTKP (break-things-kill-people) to evaluate its cost and make a pre-assumption of probability of such event [29].

Here we portray a combination of the different paths that can be followed to achieve our root goal. The pure cyber path that is focused on compromising SCADA communication system is taken from [20] with some adjustments to finalise the goal, using Aurora Vulnerability [32] as a point of inspiration. The information-technology scenario that consists of a mix of cyber nodes and physical means uses CCTV system as a main objective of the attack for its cyber components. We also broaden the scenario with possibility to include an insider help to perform some steps.

For the preparation stage attackers look for all information available about the targeted systems – both physical and network topology, possibly search in Shodan for our particular power plant and find its connection to the outside world, what protocols it uses, on what operating system etc. To retrieve information about physical components and their location attackers can use insider cooperation or even drones as it was spotted before [24].

"There are two broad categories of attacks. Stage I intrusions are those designed to gain information. These are the traditional espionage efforts we've become accustomed to hearing about, where information is stolen or deleted. A Stage II attack could result in temporary loss of power, physical damage to equipment, or other types of scenarios we often hear about. It is important to note these are not trivial to accomplish. If an attacker wants to progress to a Stage II attack, during the Stage I intrusion they have to steal information specific to that industrial environment" [29].

Stage I attack can reveal more about the protocols used, their version, login credentials, access levels etc etc, it also "... can include emails; communications involving design plans; information about security assessments; emails or documents that contain passwords; and more" [35].

7.1. Sample Attack Tree For the Full Cyber Attack

Simplified attack tree includes these main steps:

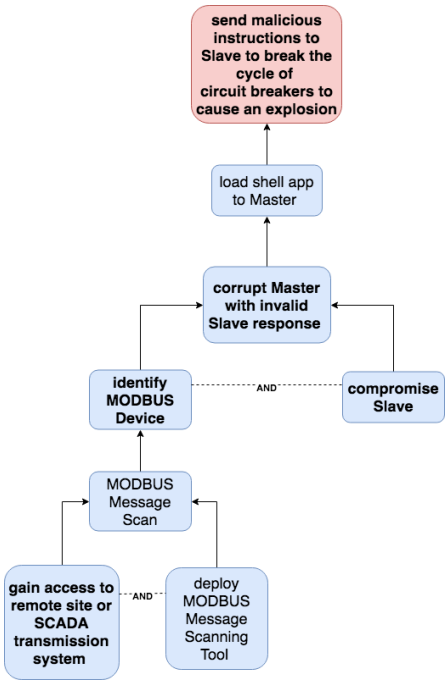

Figure 3. Simple cyber attack tree

ROOT GOAL: send malicious instructions to Slave to break the cycle of circuit breakers to cause an explosion

1. load shell app to Master

    1.1.corrupt Master with invalid Slave response

        AND

        1.1.1. identify MODBUS Device

        1.1.2. MODBUS Message Scan

            AND

            1.1.2.1. gain access to remote site / SCADA transmission

            1.1.2.2. deploy MODBUS Message Scanning Tool

    1.2.compromise Slave

Now let us have a closer look at the sub-trees of our main diagram to have a better context for understanding steps required to perform a cyber attack on a power plant. One of the main prerequisites for even being able to scan for a device that uses MODBUS protocol for communication is having access to the SCADA system:

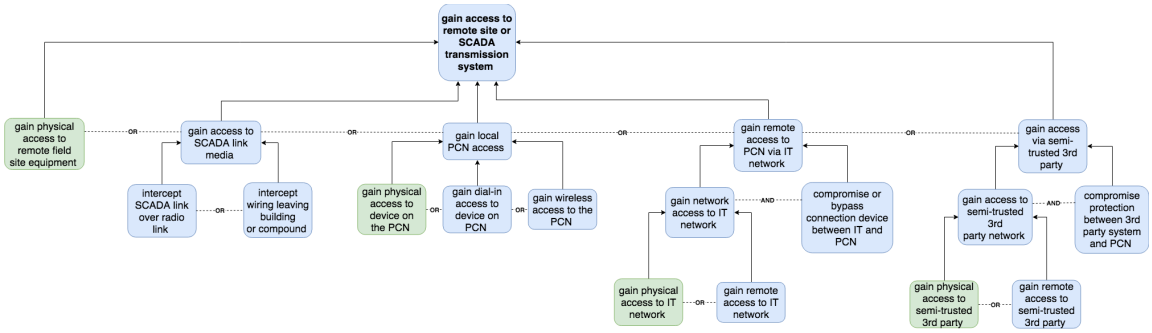

Figure 4. Access to remote site or SCADA transmission system

ROOT SUB-GOAL: gain access to remote site or SCADA transmission system
OR

1. gain physical access to remote field site equipment
2. gain access to SCADA link media

    OR

    2.1. intercept SCADA link over radio link

    2.2. intercept wiring leaving building or compound

3. gain local Process Control Network (PCN) access

    OR

    3.1. gain physical access to device on the PCN

    3.2. gain dial-in access to device on PCN

    3.3. gain wireless access to the PCN

4. gain remote access to PCN via IT network

    AND

    4.1.gain Network Access to IT network

        OR

        4.1.1. gain physical access to IT network

        4.1.2. gain remote access to IT network

    4.2. compromise or bypass connection device between IT and PCN

5. gain access via semi-trusted 3rd party

    AND

    5.1.gain access to semi-trusted 3rd party network

        OR

        5.1.1. gain physical access to semi-trusted 3rd party

        5.1.2.gain remote access to semi- trusted 3rd party

    5.2.compromise protection between 3rd party system and PCN

Here the main focus is PCN – a Process Control Network, which is a communication network that is used to transmit instructions and data between control and measurement units and SCADA equipment. In our topology main PCN servers are located in Level 3 of physical topology and we need to bypass one or two firewalls in order to get there by cyber means.

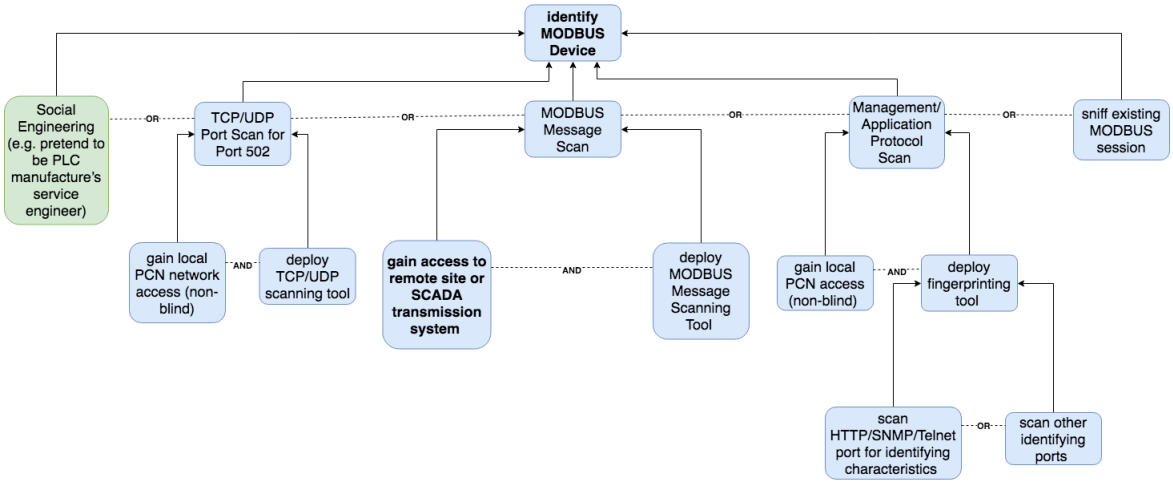

Figure 5. Identify MODBUS Device

Going further we also need to identify a MODBUS device which requires us to follow one of these paths:

ROOT SUB-GOAL: identify MODBUS Device
OR

1. social engineering (e.g. pretend to be PLC manufacture's service engineer)
2. TCP/UDP port scan for port 502

    AND

    2.1. gain local PCN network access (non-blind)

    2.2. deploy TCP/UDP scanning tool
3. MODBUS Message Scan

    AND

    3.1. gain access to remote site or SCADA transmission system

    3.2. deploy MODBUS Message Scanning Tool
4. management/application protocol scan

    AND

    4.1. gain local PCN access (non-blind)

    4.2. deploy Fingerprinting Tool

        OR

        4.2.1. scan HTTP/SNMP/Telnet port for identifying characteristics

4.2.2. scan other identifying ports

5. sniff existing MODBUS session

One of the main point of vulnerability of MODBUS protocol is the time when it was designed – power plants used to be isolated systems with the network cut from the outside world with only trusted devices connected. This paradigm has changed, but MODBUS protocol still handles its communication as if it was 20 years ago [20]. Which means no encryption and not much of filtering the instructions sent between Master (client) and Slave (server).

And last but not least – compromising the Slave server:

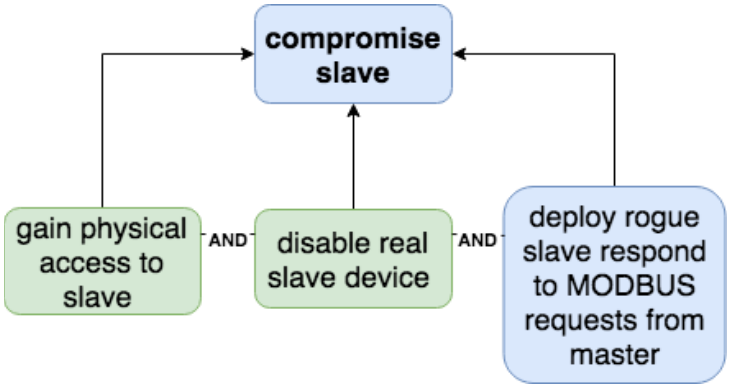

Figure 6. Compromise Slave

In total the full cyber attack tree can be seen as such:

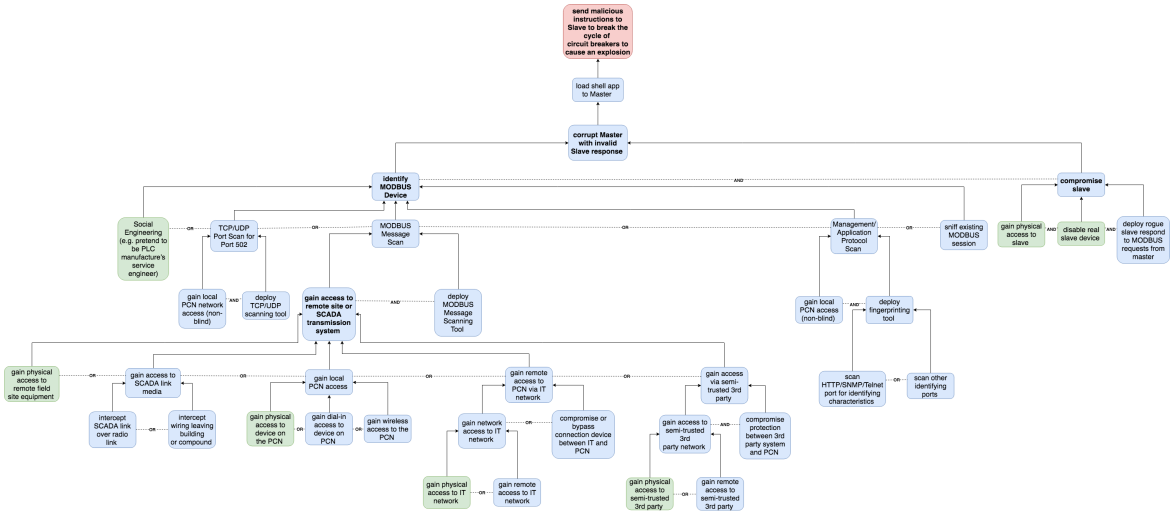

Figure 7. Full cyber attack tree

By rough estimation this scheme costs around **$5-10 millions** for attackers to perform [32]. We will take this price range as our starting point for comparison.

7.2. Sample Attack Tree for the Hybrid Attack

Combining physical and information-technology oriented means makes it both easier and harder to implement. From one side, it needs lower level of sophistication and skill set, but it also requires the attack group to be physically present at the power plant side to make things happen. It is like comparing *Diehard 4* with *Mission Impossible*.

The summary tree is presented below:

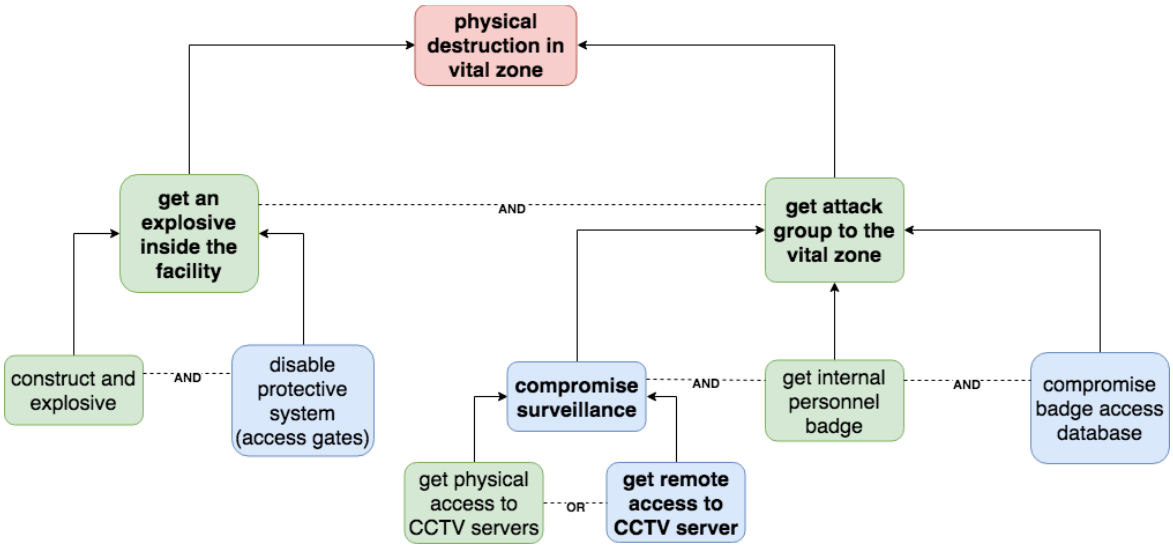

Figure 8. Simple hybrid attack tree

ROOT GOAL: physical destruction in vital zone

AND

1. get an explosive inside the facility

    AND

    1.1. construct an explosive

    1.2. disable protective system (access gates)

2. get attack group to the vital zone

    AND

    2.1. compromise surveillance

        OR

        2.1.1. get physical access to CCTV servers

        2.1.2. get remote access to CCTV server

    2.2. get internal personnel badge

    2.3. compromise badge access database

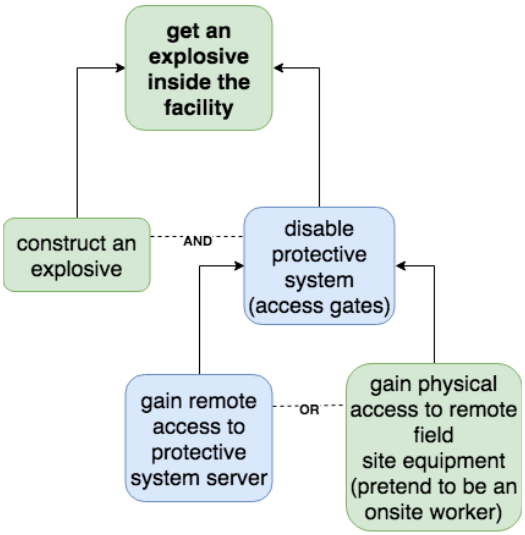

Figure 9. Get an explosive inside the facility

If we look in more details of what is required, we can see that our goal heavily depends on two main achievement point – getting the attack group and destruction materials inside the facility and making sure it reaches the deepest level, our vital zone, for the most dramatic effect. The breakdown of those sub-goals is presented below:

ROOT SUB-GOAL: get an explosive inside the facility

AND

1. construct an explosive
2. disable protective system (access gates)

    OR

    2.1. gain remote access to protective system server

    2.2. gain physical access to remote field site equipment

To be more specific about the protective systems, by it we mean mostly scan gates that make sure no restricted items or materials are brought inside the facility. We can see gates of the same purpose in other CIO such airport, the security checkpoint before entering boarding area. Those gates are located in owner-protected / general area and are highly sensitive to electromagnetic interference [41]. Being close enough physically enables attackers to disrupt its functions and give a positive light to a forbidden item and materials. Servers responsible for fetching results of security scans are also located in general area, along with CCTV servers (though they are behind two firewalls if we look at the network topology). To get this access attackers can pretend to be an onsite workers, electricians or just about anyone in the uniform!

Part of that path is also covering compromising video surveillance to make sure our group is not detected where it is not supposed to be and completes the mission. It is not only about entering the power plant, we can even say it is not about it at all – but when attackers are already in the vital zone it is going to take time to set up and detonate (or make sure it detonates remotely) the explosive material. As there are not so many people inside the critical zone, the workers' eyes can be somehow avoided, but cameras would still be

up so this part should be intercepted. Otherwise even with going through all levels, they can still get busted at the last stage of the operation.

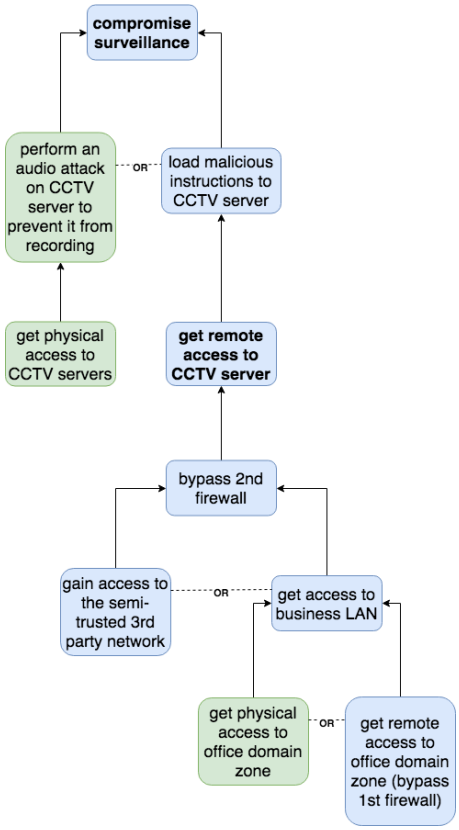

Figure 10. Compromise surveillance

ROOT SUB-GOAL: compromise surveillance

OR

1. perform an audio attack on CCTV server to prevent it from recording

    1.1. get physical access to CCTV servers

2. load malicious instructions to CCTV server

    2.1. get remote access to CCTV server

        2.1.1. bypass 2nd firewall

            OR

                2.1.1.1. gain access to the semi-trusted 3rd party network

                2.1.1.2. get access to business LAN

                    OR

                        2.1.1.2.1. get physical access to office domain zone

                        2.1.1.2.2. get remote access to office domain zone

There are couple of ways how CCTV servers and even some other not focused on recording devices can be compromised or at least be out of function for some time. One of such ways is performing an acoustic attack on the device – it requires close proximity to the servers so attackers will need to get to the general area by then. But this part is covered by other nodes that take action beforehand. “The basic principle behind this attack is that sound waves introduce mechanical vibrations into an HDD's data-storage platters. If the sound is played at a specific frequency, it creates a resonance effect that amplifies the vibration effect” [37]. Depending on the storage capacity, different frequencies are used. For example, to get 4TB HDD out of order, it will take a frequency of 9.5Hz [37]. What also comes handy – the average range of human hearing starts from 20Hz, which means that the human ear will not be able to detect this attack if low enough frequency is used. Even if there are dogs at the perimeter, they cannot hear anything below 40Hz (even though dog’s ears are more sensitive to higher pitches than humans). The reason it even works, “Because hard drives store vast amounts of information inside small areas of each platter, they are programmed to stop all read/write operations during the time a platter vibrates so to avoid scratching storage disks and permanently damaging an HDD” [37].

Another way of making sure video recordings are taken care of, is to get remote access to CCTV servers. This can be done whether by physically being onsite (which is planned anyway) or by bypassing two cyber hubs – first and second firewalls that protect CCTV servers from 3rd party network and connection to the outside world via Internet and office network. As attackers get through those hubs, the exploit it pretty much one click ahead. There has been discovered a serious vulnerability in how a camera picks up on a language interface that pretty much allows for a command line injection that can be anything. This vulnerability is present if a wide range of vendors and most of them did not show a desire to do anything about it [38]. In this case attackers do not even need to handcraft the exploit, it is available already. And a botnet created from cameras had been done already at a big scale – in 2016 around 25 000 CCTV devices became part of a botnet that performed DDoS attacks again couple of small business instances [42].

And to finalise detailed analysis of getting things done using both physical and cyber means, let us gather all the main stages that are obligatory to fulfil in order to get the attack group inside unnoticed and all the way up to the critical zone:

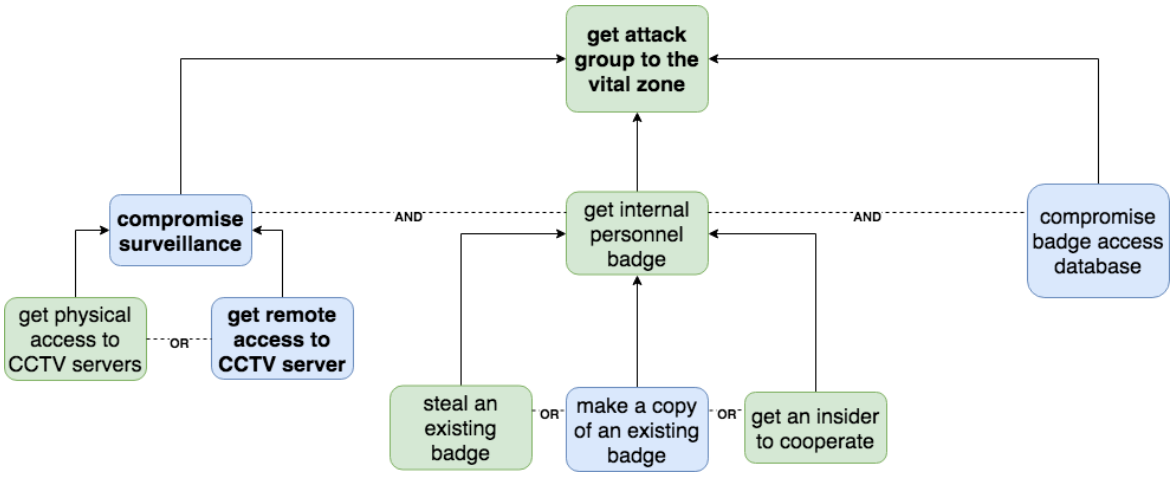

Figure 11. Get attack group to the vital zone

One way to get far is to have an internal personnel badge and make sure that is has required access level. This can be done by stealing an existing badge – and we have seen terrorist to go as far as a murder to get one – an employee of a Belgian nuclear plant was killed and his badge stolen in 2016, not so long after the airport attack [43]. Different other scenarios had already been tried out a couple of times with a varying level of success [24] but in it essence it might also mean to find out who works in the power plant, follow or stalk them, get their credentials and use those to get inside the facility. Attackers can use the original badge or make a copy of it. Both scenarios carry the risk of compromised badge being reported prior to attack, so there might be a need to copy the badge in a discreet manner or make sure that compromised worker will not have a possibility to report to anyone anymore.

A somehow easier way is to get an insider to cooperate. We would expect that employers would go through regular and random background screenings but that firstly is not always the case and also gives us certainty to only some level but we can never guaranty if a person turns. “In 2012 two employees at the country’s Doel nuclear power station left Belgium to fight in Syria. ... And earlier this year (2016) authorities investigating the Paris attacks discovered video surveillance footage of a Belgian nuclear official in the home of one of the Paris suspects” [39].

Insider is a wildcard in many senses. We can never predict how this person will behave, what motivates them, to which part and to what extent can he or she be dedicated, will there be a moment that conscious or fear catches up with them and turns the whole operation to dust. It is also unknown how much (if anything) insider can ask for the service. Some can do it driven by their believes, some can be blackmailed or threatened into this and some indeed can just ask for money. Therefore we do not include “price” of an insider in our calculations.

As we mentioned before, even with the badge or help of an insider, we still need to make sure that we can pass to the needed level using that badge. To achieve that the access databases should be compromised as well. Those databases contain corresponding information about badge authentication and biometric data of employers that it checks when they try to pass to the critical zone. As those servers are located together with other protection systems, it will take attackers the same steps as getting remote access to CCTV server – so we do not stop on this now.

Combining it all together our compiled attack tree for a hybrid approach looks like this:

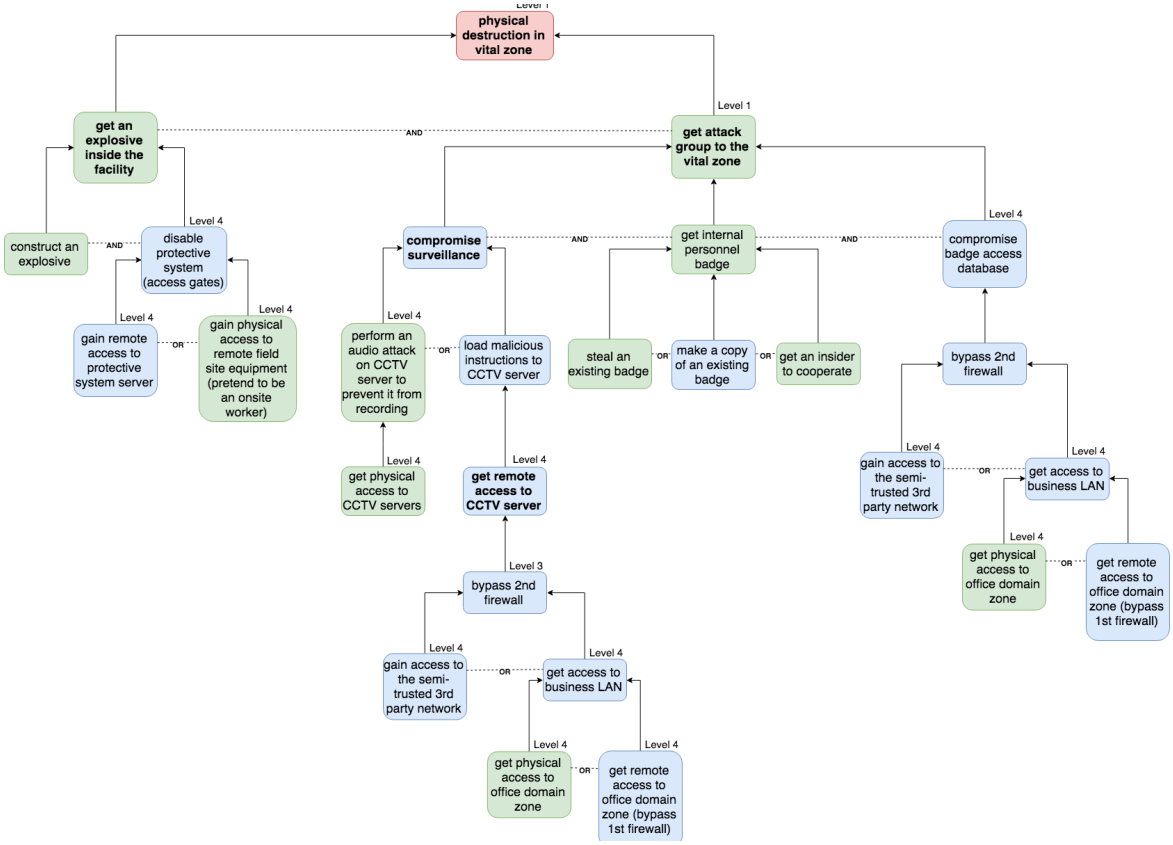

Figure 12. Full hybrid attack tree

Even visually we can see that cyber and physical nodes are pretty balanced – it takes combined effort to achieve the end result.

8. Result Calculations

Here we present the results of our findings regarding the cost of our nodes with a few annotations and explanation – context is important. The cost calculations are based on a function presented in section 5.2 of this research. We look at the cost of each of our leaf and depending on nodes relations calculate the price of the sub-goals, which also might include some additional cost involved with the sub-goal itself, excluding cost of the repetitive paths. Highlighted attack nodes are sub-goals detailed below or above. Defined price depends on level of sophistication required for a certain action and is taken in range of offers to provide such service. The best way to cover cost of the cyber components is to see how much targeted exploit kits are priced on a market.

“Quick definition: exploit kits (EKs) are programs that find flaws, weaknesses or mistakes in software apps and use them to gain access into a system or a network” [45].

Depending on complexity exploit kits can cost from $80 to $100 USD per day, $500 to $700 USD per week, and $1,400 to $2,000 USD per month [44]. It takes around 6-12 months or more to prepare the cyber part of the attack [28], part of this preparation is also researching the targeted system (via Shodan queries or other means) and then developing an exploit kit. Taking into account high profile of the target, the exploit kit that attackers would need to penetrate firewalls and protective systems to get to CCTV server and/or badge scan we would focus on the high end of the pricing – $1,400 to $2,000 USD per month which ends up being from $8,400 to $24,000 USD in total (also keeping in mind that some systems such as biometric authentication requires higher level of sophistication).

Talking about our physical component, the World Trade Center bomb used in 1993 cost only $400 USD to construct [2]. Even if we take into account inflation, it is still only around $690 USD [46]. The attack group will most certainly need two or three of such explosives to cause a significant damage bringing total cost of explosives to $1380 USD.

We assume that our attack group does not have by default needed skills to use the exploit along with performing a proper Stage I attack and target system research. Also important to mention that some cyber components would need to be performed on the spot – which means things need to be done fast and correct, plus under pressure. So it is very likely that one-two specialists are required as an external resource to be hired as a part of the group. The average salary of IT specialist is $59,072 USD a year (depending on the area of competence and country) [47]. We also need to keep in mind that this number only goes for a legal work so “the terrorist organisation planning to hire the computer professionals would have to increase those figures from three to five times, if not more” [2]. Preparing this kind of attack can take up to six months (or even twelve for some stages as getting through biometric scan systems) [28]. So for the taken 6-12 month of intense and illegal work to compromise critical systems of a power plant attackers would have to pay around $90,000–$300,000 USD per specialist. This is added to our cyber components. If at least one leaf has a need for cyber means (AND relation), we include the price of combined $180,000–$600,000 USD to the whole branch to reflect paycheque of two hired IT specialist, but we treat this number as a constant, meaning that even if the branch has more than one cyber leaf, it cost is still covered by $180,000–$600,000 USD, it does not multiply itself because we expect those specialisti to have qualification and agree to perform all needed actions to ensure that IT part is covered.

As for attackers to be near the power plant and eventually inside it is not enough to just compromise surveillance but they also need to make sure that they will not look suspicious to actual employees. This is easily resolved by using a uniform – electrician, maintenance etc. On average this can cost from $100 to $300 USD for the clothing and small parts of equipment.

To compromise CCTV server through acoustic attack does not cost any significant amount of money as the attackers just need to produce and play the sound at a concrete frequency.

Getting an internal badge varies in price. For example, to make a copy costs around $700 USD, and the instructions for making and using a device to do that are easily found online [49]. We evaluate stealing an existing badge at the same price as this point has a lot of uncertainty attached to it and may require spending on travelling, stalking the personnel, driving here and there to different locations etc, so there are a lot of indirect costs.

All prices in the table are in USD. Sub-goals marked with (*) have additional costs involved besides the combination of their leaves.

Table 1. Node price calculations

SUB-GOAL	RELATION	ATTACK NODES	PRICE (NODES)	PRICE (TOTAL)
disable protective system (access gates)* *(adds cyber)*	OR	gain remote access to protective system server	188 400 – 624 000	188 500 – 624 300
		gain physical access to remote field site equipment (pretend to be an onsite worker)	100 – 300	
get an explosive inside the facility	AND	**disable protective system (access gates)**	188 500 – 624 300	189 880 – 625 680
		construct an explosive	1380	
get access to business LAN	OR	get remote access to office domain zone (bypass 1st firewall)	180 000 – 600 000	100 – 300
		get physical access to office domain zone	100 – 300	
bypass 2nd firewall* *(adds cyber)*	OR	gain access to the semi-trusted 3rd party network	180 000 – 600 000	180 100 – 600 300
		get access to business LAN	100 – 300	
perform an audio attack on CCTV server to prevent it from recording	AND	get physical access to CCTV servers	100 – 300	100 – 300

load malicious instructions to CCTV server	AND	**get remote access to CCTV server**	188 500 – 624 300	188 500 – 624 300
compromise surveillance	OR	**perform an audio attack on CCTV server to prevent it from recording**	100 – 300	100 – 300
		load malicious instructions to CCTV server	188 500 – 624 300	
get internal personnel badge	OR	steal an existing badge	700	700
		make a copy of an existing badge	700	
		get an insider to cooperate	N/A	
compromise badge access database	AND	**bypass 2nd firewall**	188 500 – 624 300	188 500 – 624 300
get attack group to the vital zone	AND	**compromise badge access database**	188 500 – 624 300	189 300 – 625 100
		get internal personnel badge	700	
		compromise surveillance	100 – 300	

To see the final result we now need to combine prices of two main nodes of our hybrid attack tree – ”get attack group to the vital zone” and “get an explosive inside the facility” (minus duplicating IT assistance of $188,500 – $624,300 USD that includes IT professionals services and exploit kit).

In total the price for performing this type of attack is in a range of **$190,600 – $626,480 USD**.

9. Conclusions

In the end we now try to answer the question “so what?”. We looked at the pure cyber path, as it is the main option many researchers consider when they talk about future possible threats to the critical infrastructure, but we also presented a new way of thinking about the attack vector – the hybrid path. We complemented the cyber scenario with the physical actions that simplified the operation and lowered sophistication level of the skill set and also reduced preparation time from 3-5 years [32] to almost 6 months [28]. We now see that the price comparison is a definite win on the hybrid side – with $5-10 millions USD needed to perform full cyber attack that could cause a physical damage, hybrid achieves the same effect with $200,000 – $700,000 USD. It is not even about the precise number anymore, we can already see the huge jump from millions to thousands and this might be enough to take this new approach into consideration when planning an attack on a power plant.

Another question rises, will it actually happen in any foreseeable future? Frankly, still using a van to smash into the crowded street is way cheaper, takes less time to prepare and less resources to spend. And definitely reaches people at a bigger scale. Nice Attack that happened during Bastille Day celebrations in 2016 is still fresh in memory [50], but Ukrainian power plant outrage is known to a very narrow public which includes people affected and specialists in the field of security. Even though it has happened twice.

So we can make a conclusion that maybe this will not become a go-to approach in the next couple of years, but with tools becoming cheaper and skills achieved easier, that day comes closer and closer. Already now, in 2018, this type of attack is cheap enough for a main known attack organisations such as ISIL and Hezbollah, and they have even claimed or tried to attack power plants in the past – recent attempt of a physical attack on Iraq power plant in 2017 by ISIL killed nearly 12 people [51]. This plate is definitely boiling.

10. References

[1] "power plant. (n.d.)," in Collins English Dictionary – Complete and Unabridged, 12th Edition 2014. [Online]. Available: http://www.thefreedictionary.com/power+plant. Accessed: Nov. 28, 2016.

[2] G. Giacomello, "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism," Studies in Conflict and Terrorism, pp. 387–408, Mar. 2004.

[3] M. Convey, "Reality Check: Assessing the (Un)Likelihood of Cyberterrorism," in Cyberterrorism, T. M. Chen, L. Jarvis, and S. MacDonald, Eds. Springer, 2014, pp. 103–121.

[4] T. R. Ingoldsby, Attack Tree-based Threat Risk Analysis. Canada: Amenaza Technologies Limited, 2013.

[5] J. J. Andersson and T. Tardy, "Hybrid: what's in a name?," European Union Institute for Security Studies, Oct. 2014.

[6] T. M. Chen, "Cyberterrorism After Stuxnet," Strategic Studies Institute and U.S. Army War College Press, Jun. 2014.

[7] M. Stohl, "Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?," Crime Law and Social Change, Dec. 2006.

[8] "Nuclear Power Plant Security and Access Control", Nuclear Energy Institute, 2017. [Online]. Available: https://nei.org/Master-Document-Folder/Backgrounders/Fact-Sheets/Nuclear-Power-Plant-Security-and-Access-Control. Accessed: Mar. 9, 2017.

[9] "Sniper Attack On Calif. Power Station Raises Terrorism Fears", NPR.org, 2017. [Online]. Available: http://www.npr.org/sections/thetwo-way/2014/02/05/272015606/sniper-attack-on-calif-power-station-raises-terrorism-fears. Accessed: Mar. 9, 2017.

[10] A. Brown, "TERROR THREAT: UK Power Stations 'at risk' from DEADLY nuclear ATTACK", Express.co.uk, 2017. [Online]. Available: http://www.express.co.uk/lifestyle/science-technology/609929/Power-Plant-Nuclear-Attack-UK-Cyber-Terrorist. Accessed: Mar. 9, 2017.

[11] Plant Network Security. (2014). Yocogawa Whitepaper.

[12] Leyden, J. (2001). Virus toolkits are s'kiddie menace. [online] Theregister.co.uk. Available at: https://www.theregister.co.uk/2001/02/21/virus_toolkits_are_skiddie_menace/ Accessed: 31 Oct, 2017.

[13] Peterson, A. (2016). Hobbyist hackers probably caused Friday's Internet meltdown, researchers say. [online] Washington Post. Available at: https://www.washingtonpost.com/news/the-switch/wp/2016/10/26/hobbyist-hackers-probably-caused-fridays-internet-meltdown-researchers-say/ [Accessed 31 Oct. 2017].

[14] Kirk, J. (2012). Concern Rises Over the Capabilities of Anonymous Hacktivists. [online] PCWorld. Available at: https://www.pcworld.com/article/251129/concern_rises_over_the_capabilities_of_anonymous_hacktivists.html [Accessed 31 Oct. 2017].

[15] Vocabulary.com Dictionary, (2017). [online] Available at: https://www.vocabulary.com/dictionary/terrorist%20group [Accessed 3 Nov. 2017].

[16] Vick, K. (2016). ISIS Attackers May Have Targeted Nuclear Power Station. [online] Time. Available at: http://time.com/4271854/belgium-isis-nuclear-power-station-brussels/ [Accessed 14 Feb. 2018].

[17] Kopeć, R. (2013). The Threat of Mega-terrorism: Availability, Inhibitors and Motivation. Pedagogical University in Krakow, pp.105-125.

[18] Hemakumara, GPTS, "Cost-benefit analysis of proposed Godagama development node under the Greater Matara development planning program," International Research Journal of Management and Commerce, 4(9), pp. 9-19, 2017.

[19] O'Farrell, R. (n.d.). Advantages & Disadvantages of Cost Benefit Analysis. [online] Smallbusiness.chron.com. Available at: http://smallbusiness.chron.com/advantages-disadvantages-cost-benefit-analysis-10676.html [Accessed 15 Feb. 2018].

[20] Byres, E., Franz, M. and Miller, D. (2004). The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems. [online] Available at: https://www.researchgate.net/publication/228952316_The_use_of_attack_trees_in_assessing_vulnerabilities_in_SCADA_systems [Accessed 15 Feb. 2018].

[21] Wei, W. (2018). Russian Scientists Arrested for Using Nuclear Weapon Facility to Mine Bitcoins. [online] The Hacker News. Available at: https://thehackernews.com/2018/02/supercomputer-mining-bitcoin.html [Accessed 15 Feb. 2018].

[22] Shodan.io. (2018). SCADA systems online - Shodan report. [online] Available at: https://www.shodan.io/report/EM85BqkA [Accessed 11 Mar. 2018].

[23] Exploits.shodan.io. (2018). Shodan Exploits. [online] Available at: https://exploits.shodan.io/?q=SCADA [Accessed 11 Mar. 2018].

[24] Kentish, B. (2016). Nuclear power plants vulnerable to hacking attack in 'nightmare scenario', UN warns. [online] The Independent. Available at: http://www.independent.co.uk/news/world/nuclear-power-plants-vulnerable-hacking-attack-cyber-nightmare-united-nations-a7479546.html [Accessed 12 Mar. 2018].

[25] Ward, M. (2017). Power firms alerted on hacker threat. [online] BBC News. Available at: http://www.bbc.com/news/technology-40766757 [Accessed 12 Mar. 2018].

[26] Williams, K. and Bennett, C. (2016). Why a power grid attack is a nightmare scenario. [online] TheHill. Available at: http://thehill.com/policy/cybersecurity/281494-why-a-power-grid-attack-is-a-nightmare-scenario [Accessed 12 Mar. 2018].

[27] Gjelten, T. (2013). The Next Disaster Scenario Power Companies Are Preparing For. [online] NPR.org. Available at: https://www.npr.org/sections/alltechconsidered/2013/08/15/212079908/the-next-disaster-scenario-power-companies-are-preparing-for [Accessed 12 Mar. 2018].

[28] Zetter, K. (2016). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. [online] WIRED. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [Accessed 13 Mar. 2018].

[29] Dunietz, J. (2017). Is the Power Grid Getting More Vulnerable to Cyber Attacks?. [online] Scientific American. Available at: https://www.scientificamerican.com/article/is-the-power-grid-getting-more-vulnerable-to-cyber-attacks/ [Accessed 15 Mar. 2018].

[30] Cox, J. (2016). The Malware That Led to the Ukrainian Blackout. [online] Motherboard. Available at: https://motherboard.vice.com/en_us/article/wnx5yz/the-malware-that-led-to-the-ukrainian-blackout [Accessed 19 Mar. 2018].

[31] Walker, D. (2014). 'Havex' malware strikes industrial sector via watering hole attacks. [online] SC Media US. Available at: https://www.scmagazine.com/havex-malware-strikes-industrial-sector-via-watering-hole-attacks/article/538721/ [Accessed 19 Mar. 2018].

[32] Meserve, J. (2007). Staged cyber attack reveals vulnerability in power grid. [online] Edition.cnn.com. Available at: http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText [Accessed 22 Mar. 2018].

[33] Perlroth, N. (2017). Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say. [online] Nytimes.com. Available at: https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html?_r=0 [Accessed 24 Mar. 2018].

[34] Eilperin, J. and Entous, A. (2016). Russian operation hacked a Vermont utility, showing risk to U.S. electrical grid security, officials say. [online] Washington Post. Available at: https://www.washingtonpost.com/world/national-security/russian-hackers-penetrated-us-electricity-grid-through-a-utility-in-vermont/2016/12/30/8fc90cc4-ceec-11e6-b8a2-8c2a61b0436f_story.html [Accessed 24 Mar. 2018].

[35] Sheth, S. (2017). Hackers breached a US nuclear power plant's network, and it could be a 'big danger'. [online] Business Insider. Available at: http://www.businessinsider.com/nuclear-power-plant-breached-cyberattack-2017-6 [Accessed 24 Mar. 2018].

[36] Answers.microsoft.com. (2018). Possible Windows Update Virus 2018. [online] Available at: https://answers.microsoft.com/en-us/windows/forum/windows_10-update/possible-windows-update-virus-2018/a14f9f54-f25f-4b17-9bdc-92c4c025d2de [Accessed 5 Apr. 2018].

[37] Cimpanu, C. (2017). Acoustic Attacks on HDDs Can Sabotage PCs, CCTV Systems, ATMs, More. [online] BleepingComputer. Available at: https://www.bleepingcomputer.com/news/security/acoustic-attacks-on-hdds-can-sabotage-pcs-cctv-systems-atms-more/ [Accessed 8 Apr. 2018].

[38] Kerneronsec.com. (2016). Remote Code Execution in CCTV-DVR affecting over 70 different vendors. [online] Available at: http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html [Accessed 8 Apr. 2018].

[39] Macfarlane, A. (2016). How to protect nuclear plants from terrorists. [online] The Conversation. Available at: https://theconversation.com/how-to-protect-nuclear-plants-from-terrorists-57094 [Accessed 8 Apr. 2018].

[40] Terrorism and the electric power delivery system. (2012). 1st ed. Washington, D.C.: National Academies Press, pp.2-4.

[41] Johnson, D. (n.d.). Electrical Interference. [online] Tekneticsdirect.com. Available at: https://www.tekneticsdirect.com/the-tek-files/electrical-interference [Accessed 17 Apr. 2018].

[42] Cid, D. (2016). Large CCTV Botnet Leveraged in DDoS Attacks. [online] Sucuri Blog. Available at: https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html [Accessed 17 Apr. 2018].

[43] Rudaw.net. (2016). Report: security guard at Belgian nuclear plant killed, badge stolen. [online] Available at: http://www.rudaw.net/NewsDetails.aspx?pageid=203876 [Accessed 17 Apr. 2018].

[44] Rowley, O. (2017). Analysis: Pricing Of Goods And Services On The Deep & Dark Web. Flashpoint.

[45] Zaharia, A. (2016). How Automation is Changing Cyber Crime: Exploits as a Service. [online] Heimdal Security Blog. Available at: https://heimdalsecurity.com/blog/exploit-kits-service-automation-changing-face-cyber-crime/ [Accessed 18 Apr. 2018].

[46] In2013dollars.com. (2018). $400 in 1993 → 2018 | Inflation Calculator. [online] Available at: http://www.in2013dollars.com/1993-dollars-in-2018?amount=400 [Accessed 18 Apr. 2018].

[47] Payscale.com. (n.d.). IT Professional Salary. [online] Available at: https://www.-payscale.com/research/US/Job=IT_Professional/Salary [Accessed 18 Apr. 2018].

[48] Electrician Training Hub. (n.d.). Electrician Safety Clothing | The Electrician Training Hub. [online] Available at: http://electriciantraininghub.com/how-to-become-an-electrician/safety-clothing/ [Accessed 18 Apr. 2018].

[49] https://www.youtube.com/watch?v=cxxnuofREcM. (2016). [video] [Accessed 18 Apr. 2018].

[50] BBC News. (2016). Attack in Nice: What we know. [online] Available at: http://www.bbc.com/news/world-europe-36801671 [Accessed 22 Apr. 2018].

[51] Aljazeera.com. (2017). ISIL suicide attack on Iraq power plant kills seven. [online] Available at: https://www.aljazeera.com/news/2017/09/isil-suicide-attack-iraq-power-plant-kills-170902143706476.html [Accessed 22 Apr. 2018].

Appendix

I. Table of abbreviations and terms

BTKP – Break Things Kill People

CBA – Cost Benefit Analysis

CCTV – Closed-Circuit Television

CIO – Critical Infrastructure Object

DDoS – Distributed Denial of Service

EK – Exploit Kit

ISIL – Islamic State of Iraq and the Levant

PCN – Process Control Network

SCADA – Supervisory Controls and Data Acquisition

VTS – Versatile Terminal Service application

WSUS – Windows Server Update Services

II. List of Figures and Tables

III. License

Non-exclusive licence to reproduce thesis and make thesis public

I, **Valeriia Avramenko**,

(*author's name*)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

   1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

   1.2. make available to the public via the web environment of the University of Tartu, including via the DSpace digital archives until expiry of the term of validity of the copyright,

of my thesis

Cost-Benefit Analysis of a Hybrid Terrorist Attack on a Power Plant,

(title of thesis)

supervised by Hayretdin Bahşi and Raimundas Matulevičius,

(supervisors's names)

2. I am aware of the fact that the author retains these rights.

3. I certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **21/05/2018**