energies

MDPI

Perspective

Drones are Endangering Energy Critical Infrastructure, and How We Can Deal with This

Akhilesh Kootala [1], Ahmed Mousa [2] and Philip W. T. Pong [3,*]

[1] Department of Mechanical and Industrial Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA
[2] Utility of the Future, Public Service Electric and Gas Company (PSE&G), Newark, NJ 07102, USA
[3] Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA
* Correspondence: philip.pong@njit.edu; Tel.: +1-973-596-3533

Abstract: Drones are becoming a greater threat to modern electrical grids with the capability to cause expensive and time-consuming damage repairs to substations and transmission lines. Consumer drones have the potential to cause harm at a low cost, and finding methods to counter these threats is becoming more crucial to keep grids secure. In 2021, there was an attempted attack on a substation with a consumer drone which highlighted the need for research in this area. Previously, there has been a large focus on counter drones around places such as airports; however, more focus is warranted to analyze drone impact on the grid infrastructure. Methods to counter drones' harmful impacts vary from physical methods to using electromagnetic waves. This article looks to identify and propose potential applications for existing technologies, as well as developing anti-drone technologies. These methods have not been adopted yet; thus, there is a great opportunity to utilize these existing technologies to defend the grid. The methods investigated were surveillance cameras, patrolling drones, nets, signal jammers, and energy weapons. The existing technology is currently lacking in the area of drone defense and can be improved with existing studies. However, there is a need to identify those methods and find ways to apply them to the power grid. Different defending technologies vary concerning their potential implementation. This paper also identifies and categorizes different results these methods produce to counter drones and their associated costs.

Keywords: drone; defense; security; infrastructure; utilities; transmission; substation

Citation: Kootala, A.; Mousa, A.; Pong, P.W.T. Drones are Endangering Energy Critical Infrastructure, and How We Can Deal with This. *Energies* **2023**, *16*, 5521. https://doi.org/10.3390/en16145521

Academic Editor: Abu-Siada Ahmed

Received: 27 March 2023
Revised: 7 July 2023
Accepted: 8 July 2023
Published: 21 July 2023

1. Introduction

With the increasing prevalence of consumer drones, an uptake in the use of drones to conduct attacks against critical national infrastructure has followed. From airports to power grids, many different components of vital infrastructure are being threatened and targeted by drones, with the matter growing increasingly more urgent as drone technologies advance [1]. Drone attacks and disruptions around airports have existed for years [2]. An attack on a substation in July 2020 [3] demonstrated for the first time how a drone can be used to deliberately damage energy infrastructure. This attack involved a DJI Mavic 2 drone equipped with a camera and memory card, with other identifying markings removed to prevent tracking. This consumer drone costs around 800 dollars [4], and similar drones with cameras can be purchased for much less, with the cheapest ones ranging from 30 to 90 dollars [5]. Figure 1 below shows an example of a consumer drone. The drone also had a cable with a copper wire attached intended to create a short circuit at the substation. While this attack was not successful, the risk it posed was high. Attacks like these have the potential to disrupt grid operations and cause harm to substations and transmission lines [6], disruptions that could lead to power outages, expensive repairs, and unsafe conditions around the energy infrastructure. With the threat of physical attacks on the grid being high [7,8], the likelihood of drone attacks like these is increasing [9]. As the barrier of

entry to launch a devastating drone attack is so low, with drones being inexpensive and easy to purchase from retail stores and online retailers, the need to protect against these attacks is of great importance. In addition to the up-front dangers of this problem, the ability to track consumer drones back to their owners is difficult. New technology and methods to prevent and minimize attacks and damages are needed to properly combat the threat posed by drones to critical energy infrastructure.

Figure 1. Model of a typical quadcopter. Image from Creative Commons.

The task of protecting the power grid can be compared to protecting other types of critical national infrastructure. Critical national infrastructure (CNI) is any infrastructure that is vital to the point that if it was harmed, it would have a debilitating effect on a country's security, economy, public health, safety, or any combination of these factors [10]. When it comes to protecting critical national infrastructure, there are many barriers to guarding them against threats, the largest one being the vast size of these systems, making it nearly impossible to fully protect against all threats. To make the different aspects of the United States' extensive power grid easier to comprehend, its electricity transmission system can be broken into two major parts: substations and transmission lines. Transmission lines can be compared to railroads in that they both span very large distances and go through various environments, and substations can be compared to train stations in that they are centrally located. Similar to how it is very difficult to protect all of the thousands of miles of railroad that stretch across the country, it is also an imposing task to shield the 700,000 circuit miles of transmission lines in the U.S. [11]. This means that stopping a drone from attacking a specific area of the transmission line without prior knowledge of the attack's location is next to impossible without specialized safeguards in place. If a drone was piloted into a transmission line located in a rural area, then significant damage could be caused without the individual conducting the attack having to fear detection, both before and after the fact. However, when looking at substations, this problem is nonexistent. Similar to train stations, their centralized location makes them easier to defend against drone attacks; although, without efforts taking place to specifically target drones, even these places are still vulnerable. Due to the inherently difficult nature of protecting them, this paper will focus on transmission lines. There are several challenges associated with protecting transmission lines, such as monitoring the large footprint they cover, detecting drones as they approach, and how to address the drone threat once it is found. Additionally,

it is hard to immediately stop a drone once it is detected. As such, solving this problem is another area of focus.

In this report, we realize that stopping an attack while it is happening might not be feasible to do on a scale such as that of the power grid; however, we seek to propose ideas regardless of current feasibility since much is unknown in the field. Our solutions will also differ in focus. Solutions presented will range from those that will most functionally protect the grid from disruptions regardless of price, to more cost-effective approaches that seek to implement cohesive protection while minimizing expenditures. For transmission line protection, we investigated plans from the federal government on defending infrastructure such as hydroelectric dams and railroads. Through this, we found that there are a variety of technologies that can be applied to mitigate the effects of transmission line damage. These technologies are in various stages of development and use but all have the potential to be applied to the grid.

From the analysis, this paper can conclude that security is lacking in current power grids and can be improved with existing and researched technologies. From this research, no existing ways to protect the grid were found. However, because of this, looking into other areas and related fields was the next step for finding related problems. Through this search, many solutions were found that could be adapted to defend the grid. There is not currently a clear answer as to which solutions are the most effective and how to measure their effectiveness and costs. This paper put forth a framework to analyze the technologies explored; however, there needs to be more work done to make more accurate cost and effectiveness calculations since there is not enough data to judge their use on a grid. Currently, none of the technologies mentioned are being used or have been tested to protect the power grid. However, there are plans to delve into how they can be applied differently to fit the grid.

2. Methodology

To research the field, the first step was to search for solutions to this problem in two ways. This includes strategies to protect other critical national infrastructure and methods to apply them with. First, we investigated critical national infrastructure and looked to see if drones were a problem with other forms of CNI. Then expanding the search was the next goal to see what other threats affected infrastructure and if so, what procedures already existed to protect them. From this search, it was found that airports have the closest relationship with consumer drone risks and past threats. Then, the next step was looking into existing methods to defend against drones, including military technologies in consideration of all methods that were being developed to target drones, since military companies have developed a lot of technology to counter them. The types of sources used to gather the information were research papers, news articles, military contractor material on drone defense, and commercial websites and blogs when necessary to find information such as product prices or specifications (Table 1). With the information collected, it was found there were no methods currently employed on power systems to protect them, and the technical information was used, if available, to identify and recommend potential implementations of the researched technologies on a power grid.

Table 1. Research Areas.

Research Areas	
Forms of CNI	**Anti-Drone Technology**
• Hydroelectric Dams • Airports • Rail Network • Public Water Systems	• Drone Jammers • Directed Energy Weapons • Net Guns • Surveillance Cameras • Patrolling Drones

3. Relevant Works

There are currently no existing methods to defend substations and transmission lines against drone attacks, as they are a relatively new threat. Methods to fight drones in general have not been applied to a power grid, and many current methods have some downsides when looking into power grid implementation. The ways they deal with drones involve a full takedown of the drone during flight or reacting after an attack has been discovered and reducing the impacts. While physically eliminating a drone is an effective solution to remove drone attacks, the potential collateral damage caused by an out-of-control and falling drone is high. There is also a high risk of interference with grid equipment since many methods to disable drones involve using electromagnetic waves that are also utilized by the grid for various functions and communication [12].

Manually detecting a drone visually or using a system of sensors to identify and track a drone are existing methods for drone detection. Currently, drone detection relies on a drone attack being reported by someone or through a visual inspection by a troubleshooter once a problem is noticed in the control room. The transfer of information with this method is very slow and can be easily improved with more effective surveillance.

The FAA has seen an increase in drones around airports and is experimenting with new technologies to mitigate them. The Ronald Reagan Washington National Airport (DCA) in Arlington, Virginia had to shut down air traffic for around 45 min in one instance of a drone flying near a runway [13]. When it comes to protecting aircraft and airports, in 2021 and 2022, the FAA at Los Angeles and Atlantic City airports had taken steps to protect airports such as through implementing various technologies to detect, track, and identify drones (DTI). By testing these new systems, the researchers hope to learn more about drones near airports and how to pair these DTI systems with navigation and communication systems that are already adopted at airports.

Regarding other types of critical national infrastructure, there have been different ways of protecting them from attacks. If there is a suspected threat, then security is elevated by adding more cameras and posting security guards at the locations of interest. These cameras can be monitored by software or personnel, which then send a notification to the security or staff. The public is also involved when it comes to security on infrastructure such as railroads and highways using the "See something, say something" program. This increases the number of potential eyes because all the people passing through are used to detect dangers. When it comes to substations, a similar process can be used. Indoor substations such as gas-insulated substations (GIS) have the benefit that they are fully covered up, making any drone attack on them impossible. However, when it comes to train tracks, there are no easy methods to protect all lines because of the immense span of the infrastructure. This means that the definition of security must be redefined to focus more on the prevention and mitigation of damage. This idea can then be used on transmission lines. It is nearly impossible to always defend every inch of a transmission line, so the focus should be on minimizing the threats and the subsequent damages of an attack if one happens.

4. Review

Some of our methods of dealing with drones range from taking them out midflight to mitigating the damage they cause. Due to the damaging consequences of taking out a drone midflight, we find that there is interest in investigating how to mitigate the adverse effects of a drone attack as well. We also investigate the benefits of increasing the detection and removal speed of drone threats on the grid. For all our recommendations, we propose a detection system using cameras, microphones, drones, or a combination of these to identify and locate drone attacks. This will allow surveillance coverage of a wide geographical range of the power lines. This system will feed information to the control room and alert the operators about possible drone attacks as fast as possible. A surveillance system of this scale on the grid does not currently exist, so this idea would have to be implemented from the ground up. Another hurdle would be developing a program that can reliably detect

and track a drone off information from sensors. While there have been investigations on how to use cameras to track drones [14,15], more work needs to be taken in this field as well because the software still needs to be optimized.

When it comes to defending the grid, there are two different qualities to examine: resilience and reliability. Resilience deals with the grid's ability to withstand low-probability and high-consequence hazards [16], and reliability is the grid's ability to withstand high-probability and low-consequence events [17]. For drone attacks, the former is the metric of focus since they are not common events and have the potential to cause significant damage. Finding out how to measure the resilience of grids and the economic costs of such attacks is a major obstacle when quantifying the effects and risks drones pose to the grid. Thus, the methods that will be discussed further will focus on improving the resilience of the power grid.

To compare all of these methods broadly, we must develop constraints for determining which technologies would be best used for different segments of transmission. There is not a one-size-fits-all solution for the transmission system because of many factors such as equipment size and geographical location. For this, we will organize the technologies into categories that determine how effective they are at minimizing disruption to the grid. There are two main categories that these methods fall into, which are attack disruption and damage mitigation.

Attack Disrupting

Drone attacks have been researched for many years in the context of warfare [18]; however, when it comes to attacks on power infrastructure, very little is known. To combat this, there should be more research on the ways attacks can be stopped. One way to look at eliminating drone attacks is to stop them either during or right before the attack happens. This is called attack disruption. Some methods mentioned to counter drones are past the research phase but when it comes to drone attacks on critical national infrastructure, these methods need to be further developed. These methods are drone jammers, directed energy weapons, and net guns.

i. Drone Jammers

Jamming the signal of the drones [19,20] is a possible way of countering drone attacks (Table 2). Jamming devices work by emitting electromagnetic noise at radio frequencies that drones operate and transmit videos at. These waves are also at a high enough power level to significantly interfere with effective communication between the drone and its pilot. The frequencies are normally set at 2.4 GHz or 5.8 GHz which are also "non-assigned" public frequencies. This means that they will not interfere with any dedicated radio bands such as that of cell phones or aircrafts [21]. While jamming devices are illegal in many parts of the world including the US, a British company in, called Drone Defense (Ordsall, England), was able to obtain special legislative approval to use drone jamming technology around a prison in the UK. The device is called SkyFence [22] and it disrupts the signals going to the drone when a drone detection system finds a drone within range of the prison. This technology has great potential for use around power infrastructure; however, there needs to be legislative action taken to make this legal in many parts of the world [23,24]. In addition, an investigation to see if jammers might interfere with grid equipment is needed.

Table 2. Drone Countering Methods.

Drone Countering Methods	
Attack Disruption	**Damage Mitigation**
• Drone Jammers • Directed Energy Weapons • Net Guns	• Surveillance Cameras • Patrolling Drones

Potential Solution

Drone jammers can also have the added benefit of not being very complex systems to operate since there are no moving parts. They can be placed on top of transmission towers to increase proximity to the wires and be customized to their environment with various radii on their jamming range if there is a lot of infrastructure along the way. A grid-wide network of jammers with a fence style and gun style can be implemented to obtain the benefits of both weapons. Transmission near other important infrastructures can use technology such as a jamming fence to protect a wide area while a jamming gun can better combat drones on wide and clear stretches of transmission lines. To help control all these jammers, there would need to be added cameras and sensors to detect and locate drones to target. In the future, research about these implementations may lead to the viability of this technology for transmission line defense.

Challenges

Regulatory approval is the largest hurdle in the way of this technology. It is proven to work against drones; however, this issue could prevent their implementation despite the ease of use this offers, and drone jammers must be tested more on the scale of transmission lines to be applied in the future. In addition, further tests need to be performed on the range of the sensors as well as on how the coverage of the jamming zone can be changed for different transmission line locations. For example, a drone jammer may provide a wide area of coverage, about 2 km [25,26]. However, with this large area, it may interfere with objects outside of the right of way where transmission lines are located. This is a consideration that must be considered in a populated area because the jammer system can interfere with technology in buildings or on people.

There are also handheld drone jammers such as the one in Figure 2 that can be used to take down drones. With the small size of these mechanisms, a modified system that is aimed at using machinery and camera sensors can be used to disable drones as well. This technology would have to be further developed; however, this system would offer a more targeted method of attack compared to a jamming fence that might be problematic in certain areas. Furthermore, the range of 1 to 2 km [27] for the gun to reach the drone makes this system potentially cheaper, as each jammer can look over a large area of the transmission line. If handheld jammers can be placed on top of transmission poles and directed at targets, then there will be less chance for interference because the area of jamming is much more targeted and not in a blanket area around the towers. However, installation on the top of transmission towers is expensive and requires outages. Faults can happen if the jammers accidentally fall. More research and development efforts are needed for this idea.

ii. Directed energy weapons

In the defense industry, companies have developed directed energy weapons to take out drones from the skies [28]. Directed energy weapon is a term for any technology using a beam of concentrated electromagnetic energy or atomic or subatomic particles. These weapons can include high-energy lasers, high-power microwave or radio waves, or a particle beam [29]. They also can inflict great damage, from cutting through metals to destroying electronics, and they also have the potential to be lethal. For use against drones, this technology can be useful to automatically identify, track, and destroy drones mid-flight. Some companies that currently produce these kinds of directed energy weapons are Lockheed Martin Corporation (Bethesda, MD, USA) [28,30], The Boeing Company (Arlington, TX, USA) [31], and Raytheon Technologies Corporation (Waltham, MA, USA) [32,33]. Raytheon has also proposed using these systems to guard against drones for public events such as the Super Bowl, so that such technology may have a use on the electrical grid [34]. However, the downside of this technology is that it is very new and there could be potential interference with devices on the grid. They would also have to maintain a line of sight the entire time because these energy beams can be blocked by certain obstacles [35].

Figure 2. SkyFence Drone Jammer. (From dronedefence.co.uk) (accessed on 1 March 2023).

Figures 3 and 4 from Boeing show their current directed energy weapon hardware and software interface.

Figure 3. Boeing Directed Energy Weapon. (From boeing.com) (accessed on 1 March 2023).

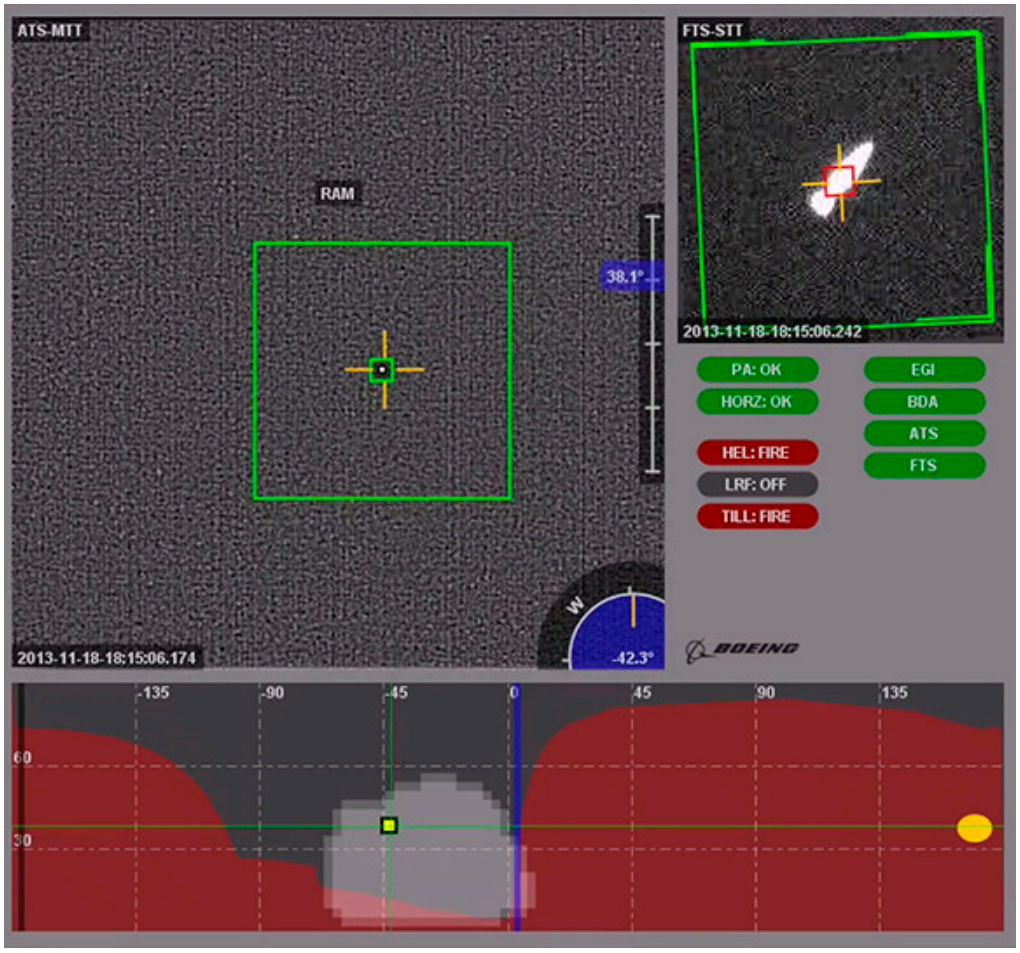

Figure 4. Boeing interface for targeting drones. (From boeing.com) (accessed on 1 March 2023).

Potential Solution

Deploying directed energy weapons to protect transmission lines is another use of this technology. By incorporating a rotation mechanism, these weapons can operate on targets from all directions. A recommended implementation of this technology, then, would be to place one of these lasers on a rotating platform that is controlled by cameras. This technology can come in the form of a turret that could theoretically be placed at the top of transmission towers. These, in combination with a drone detection system and tracker, can guide the turret to shoot down the drone. Thus, allowing the weapon to take out drones before they cause damage to the grid. This technology can also have very large effective ranges of around 20 km [36,37], so not many of these devices would need to be used to protect large expanses of transmission lines. However, this would be an expensive undertaking to set up on the scale of the grid. While this method would also stop any drones in their tracks, the cost of these directed energy weapons makes this prohibitive. They can go up to millions of dollars to develop and produce [38]; however, the exact pricing is not widely available.

This could also be implemented similarly to the drone jamming guns but instead with directed energy weapons used in these systems. The weapons could monitor wide ranges of transmission designs and keep a watch of these long stretches as well. The location of these could also be on the right of way near the transmission lines to minimize installation costs. Furthermore, because the right of way is normally clear, the line of sight between these weapons can still be maintained.

Challenges

Directed energy weapons have many similar challenges to jammers. An example of one of the challenges is how drone jammers must be tested more on the scale of transmission lines to be applied in the future. However, with this large area, it may interfere with objects outside of the right of way where transmission lines are located. This is a consideration that must be considered in a populated area because the jammer system can interfere with technology in buildings or on people. They would also have to maintain a line of sight the entire time because these energy beams can be blocked by certain obstacles [35].

Additionally, and this is potentially the most important factor, is that this technology is still in its infancy. This means that it would not be ready to be applied to the grid anytime soon and would have more years of development ahead.

iii. Net guns

The final method of neutralizing a drone threat is by shooting a net at the drone [39]. This method of tackling drones is useful against a moving target because the larger surface area of the net gives it a larger area to catch. This allows there to be less precision from the tracking and aiming systems. Net guns usually are around the size of a handheld flashlight that shoots a 3.2 m by 3.2 m net with a range of 49 ft (15 m) [40,41].

Potential Solution

Net guns can also be placed on top of transmission lines to maximize their range. They would need to be mobile and connected to machinery that can rotate and aim the net for it to be effective. This system would also have to be combined with sensors to detect and track drones for the net guns to operate.

Challenges

These systems are often human-operated and not automated. The drawbacks to this technology are that they are handheld, meaning that personnel along transmission lines would have to use it manually, and controlling where the drone falls can be difficult. A drone falling could cause some collateral damage, especially near a populated area. Figure 5 below shows an example of a handheld commercially available net gun.

Figure 5. Handheld commercially available net gun. (From netgun.com) (accessed on 1 March 2023).

There is also research into using drones to capture drones by attaching nets to them [18]. In this system, two unmanned aerial vehicles (UAVs) are connected by a net between them

and piloted to catch the target drone in the net. With this technique, the falling drone is taken out of the equation because the cooperating UAVs guide the drone down. The problems with this system are that they would have to be within the operating range of the drones and may need the aid of an operator. In addition, this system is still in the realm of research with not much data available on its application. In the future, support from a government agency such as the Department of Homeland Security may be needed to protect critical energy infrastructure.

iv. Other methods

This paper also did not go into the areas of research with using animals such as eagles to counter drones similar to what the Danish police have done [42]. While we are not going to investigate this method in this paper, it is an interesting and experimented-on method to tackle drones. They have successfully used eagles to counter drones but this also comes with many ethical questions that have not been answered yet. Moreover, this method is yet to be tested on something as large as the power grid, so there is more work to be done on its effectiveness on a large power grid.

Ethics are also a consideration with this method. This is something that also needs to be explored due to the use of animals. We are not going into ethical arguments in this paper but it seems to be a large concern of this method.

Damage mitigation

When looking to mitigate dangers, the exact parameters that will be focused on will be economic damage and grid disruptions. Any attack on the grid will incur some economic cost, so finding a method that can minimize the associated costs will be a solution. Economic costs can range from paying a crew to locate and remove the threat to purchasing cable or devices for drone damage-related repairs on the grid. Besides, any attack will interrupt the flow of energy through the powerlines, so making sure the flow of electricity is affected minimally is another focus.

i. Surveillance cameras

These are a very common technology in other areas of infrastructure so this is a very mature and developed technology. The specifics of how to connect and operate this system will be the largest question to their deployment because of the large area. The physical constraints are not too important for this technology due to its simplicity and ability to be implemented almost anywhere.

Potential solution

Surveillance cameras are one technology that can be added to the grid. They can use an IoT system of communications because this will be the best method to transmit the data from the cameras. The IoT would be integrated with smart grid technology and communication as well and be used by transmission system operators to aid in decision-making. Having the drones operate through this network will help manage all the other data from the grid. The cameras can be located on the borders of substations and on top of transmission poles.

Cameras such as the ones in Figure 6 below could be placed along the transmission infrastructure and the data could be analyzed to locate drones. They could be placed on the top of transmission towers so that they have the maximum field of view. They could also be rotated similarly to turrets so that each one can view a larger area with fewer cameras required in total. The monitoring of the cameras for drones can be done manually or with algorithms but using algorithms would be the most efficient way to do this task. There are already algorithms made to identify drones from camera footage, so the future challenges would be tuning the precision of the drone to catch and remove drones on power lines. There would also need to be infrastructure to collect and process the video data which could add up the cost and system complexity depending on the number of cameras being used, so this would also need to be a factor to be considered. This technology can be used

for providing data to operators and many of the anti-drone systems mentioned. This could decrease economic and time costs to return the service to normal.

Figure 6. Outdoor CCTV cameras. Image from Creative Commons.

Challenges

Cameras have a handful of challenges. Being on the top of transmission towers means that they can be a target for lightning. Lightning protection for these cameras will need to be carefully considered. Moreover, the data deluge may overwhelm the operators. Automatic identification algorithms will most likely be needed. There would be an extensive setup for the network of sensors and communication devices, and there would be a large cost of having more sensors also there. Having cameras deployed in this manner all over the grid is expensive to build up and install due to the scale and infrastructure needed to build, operate, and maintain them.

ii. Patrolling drones

Another one of our solutions is to use drones to fly alongside transmission lines to monitor any drone attacks. These patrolling drones could also be used to monitor transmission lines for other problems, but they would be able to locate a drone attack very quickly and efficiently. In Indonesia, specialized unmanned drones have been used for monitoring transmission lines. They can patrol at a pace of 4 transmission towers in 10 min [43]. Technology such as this could be combined with an algorithm to detect drones to have a more rapid response time. The unmanned nature means that it can be deployed and used without much manpower to monitor or control it. Figure 7 below shows a drone inspecting a powerline. In addition, using drones such as this for monitoring the grid regularly can increase the speed of detection and be useful to operators for routine diagnostics of the line. Since it takes extra time for a serviceman to drive to the site and monitor it themselves, the drone could save time with its automated traveling. The patrolling drone has the potential to be equipped with a net or hook to catch and remove the attacking drone as well. Drones with nets attached that could also be used to remove drones [17] have been researched and are a promising possibility. This would eliminate the need for a serviceman to get lifted or flown to a high-voltage line, making the drone-removal process a lot safer.

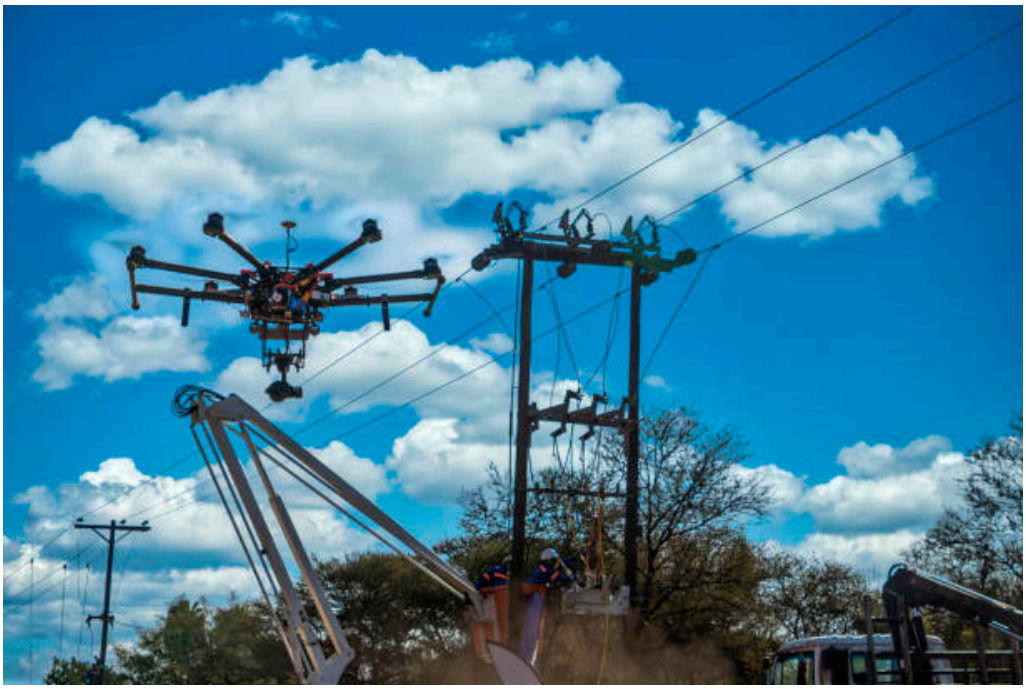

Figure 7. Drone inspecting power lines. Image from Creative Commons.

Proposed solution

For patrolling drones, there are many possible systems of controlling their operation. This system can be fully automated with communications running on an IoT system as well. This would help keep the drone connection in areas where cellular service may not exist. This is also the technology with the most success on power grids because they have been experimented on for regular maintenance. For recharging, there is experimental technology where the drone can attach itself autonomously to transmission cables to charge itself [44]. This would entirely remove the need for a drone to return to a central hub to charge and would drastically increase the operating times of the drones.

Challenges

There needs to be research done on how drones would detect other drones and how these systems would be integrated into a warning system for transmission system operators because currently, no system exists. Furthermore, the number of times a drone would need to fly over would need to be researched to find the most effective way to increase coverage of the grid. In addition to this, there is more work to be done with drone charging technology using transmission cables because this can drastically increase the operating times.

Figure 8 below adapted from a paper on autonomous patrolling drones [44] for fault detection shows the MIDRAS [45] drone used for their experiment and an adapted model for training and operating the AI. This can be adapted for drone detection and be used for its initial use case. The YOLOv4 model is their model to detect faults and they use other AI models in the inspection phase.

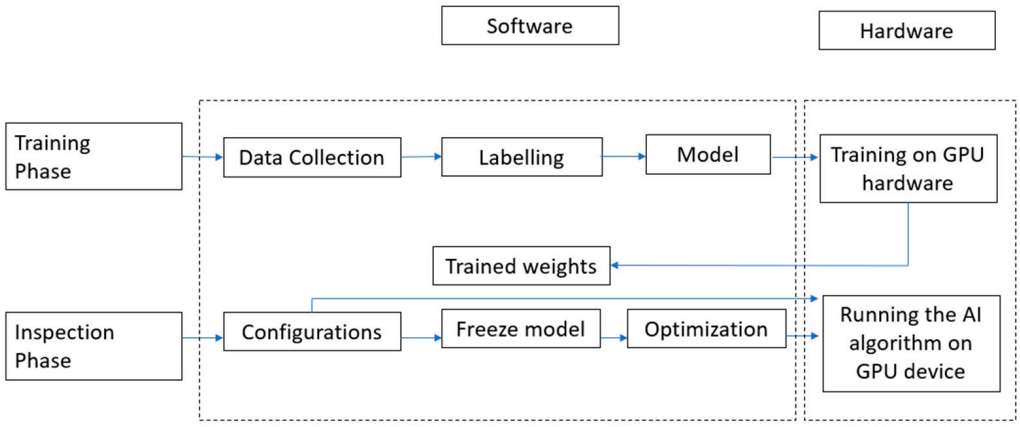

Figure 8. Model for autonomous drone adapted from [44].

5. Discussion

Focusing on minimal disruption to power delivery

Developing a system with a combination of these technologies according to the importance of a certain transmission feeder might be a better strategy. If the focus was ultimately on minimizing the effect these attacks can have on delivering power, then the best way is to increase the resiliency of the entire grid. Making sure that there is not a single point of failure or very few safeguards is necessary to achieve this; for example, avoiding the situation where a region is only supplied with one transmission feeder. If there are transmission lines that are too crucial, then more costly methods of protection can be used, such as using signal jammers or directed energy weapons, because the cost of losing these lines is too great. However, if there are lines that can be taken out without sacrificing the power supply to the rest of the grid, then a lower cost and less timely solution can be used to monitor the lines, such as an autonomous drone doing scheduled flyovers, or flying a drone only when an anomaly is detected in the control room. Using anti-drone systems as necessary to balance the costs and risk is the best method to effectively guard the grid.

For a system that focuses on minimal disruption to power delivery, the technologies that will stop a drone in its tracks such as drone jammers, directed energy weapons, and net guns are going to be the highest-rated devices. Implementing these with other technologies in future grids would be the ideal way to protect against drones. We can give these methods the highest weight due to their ability to stop attacks before any damages occur.

Economic considerations

With all these methods mentioned, there are other considerations to take into account other than the effectiveness of the technology when it comes to neutralizing a drone threat. The economic costs are another large part of the problem. While the exact economic costs of these technologies are not very well known, the costs of some of these methods can be assumed to be prohibitive since they play a great role in determining the feasibility of the method.

Focusing on minimal economic costs is a valid method of dealing with the drone threat. This would be like decreasing the disruptions an attack would cause on the grid because service disruption comes with a cost. However, the costs of implementing drone-destroying technology can often be too great depending on the implementation. Calculations should be conducted to quantify the economic costs of each type of system in comparison to each other and the existing system as well as compare them with the potential costs saved by eliminating potential attacks. This would then provide a clear idea of which methods are feasible for defending the grid.

High cost: Systems such as that of directed energy weapons are the most cost prohibitive. The exact costs for a smaller system are not known, but military systems that are capable of damaging heavy machinery such as helicopters and boats cost around 40 million

dollars [46] and are outfitted on naval ships. For this application, the size and power of the systems need to be a lot smaller but they would still probably have a significant associated cost.

Middle cost: Net guns can be bought from 500 to 3250 dollars from manufacturers [31] and these are a relatively lower-cost technology to use against drones that will not need regulatory approval. Using patrolling drones can cost a lot less than using helicopters to patrol along transmission lines [46]. This means that costs can be significantly saved using technology such as this. Helicopters can cost around 4000 dollars per day, or 2 million dollars for a utility company to fully own. Besides, there are significant costs to hire, train, and manage helicopter personnel. Eliminating the need for these steep costs will make patrolling drones a much more attractive option for finding threatening drones.

Low Cost: Other systems involved such as drone jammers have been used to counter drones, but the cost of commercial systems is relatively unknown. However, jammers can be bought online for around 50 dollars [47]. With a relatively low cost [48], this technology is a lot more feasible. Finally, camera systems can be a low-cost method of monitoring the grid. With CCTV outdoor cameras varying in cost, they can be found from 500 to 1000 dollars per camera [49,50]. However, this does not encompass the cost of the entire system. Technologies such as computers and the automatic identification algorithms needed to manage them are all costs that are currently not taken into account.

Surveillance cameras and patrolling drones also fall into this category; however, the exact costs are difficult to estimate for these systems due to a lack of information on infrastructure for these types of systems. They all come in many different forms so hardware costs can vary depending on the camera or drone chosen.

Asset values

Another area where the cost comes into play is the value of the equipment that is being targeted. For devices in a substation that can be affected by a drone attack anywhere on the transmission, the costs can be in the millions of dollars to replace a 500 kV rated transformer [51,52]. There are also costs associated with the downtime a transformer being offline will cause [53].

With all these different methods of looking at protecting the grid, the answers to how we will protect the grid in the future are not one-size-fits-all solutions. Due to the complexity of all the factors involved, the pros and cons of every method will make them useful for their special-use cases.

Recommendation

From the methods and overall decision-making matrixes we proposed, we recommend the patrolling drone on top of the other methods. This is mainly for a few reasons: cost, simplicity, and multitasking. When it comes to cost, the lack of need to build up a grid-wide network of costly machinery that needs to be constantly maintained is a large downside. Autonomous drones would need more infrastructure for connection; however, this requires much less complexity compared to other methods. In addition, they can be integrated with smart grid communications. Figure 9 below shows the diagram of how this system could be integrated. When it comes to simplicity, having the drones automated makes them very easy to use and takes away the need for extra manpower. Furthermore, this would be less infrastructure to maintain for the utilities. Finally, multitasking can be used to aid servicemen when it comes to looking at downlines and other grid problems. For utility companies today, there is a large focus on using technology to make the jobs of servicemen safer and more efficient, and this would save thousands of manhours and eliminate risk when it comes to examining high voltage cables. Figure 10 and the Tables 3 and 4 show our recommendation of methods organized by the categories of attack disruption and damage mitigation.

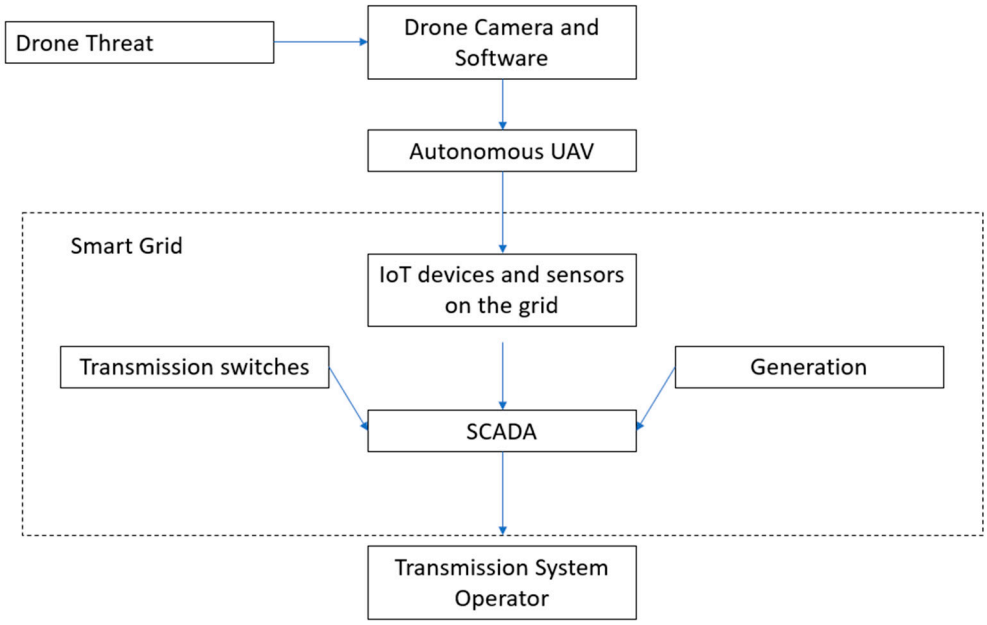

Figure 9. Model of the proposed autonomous drone system.

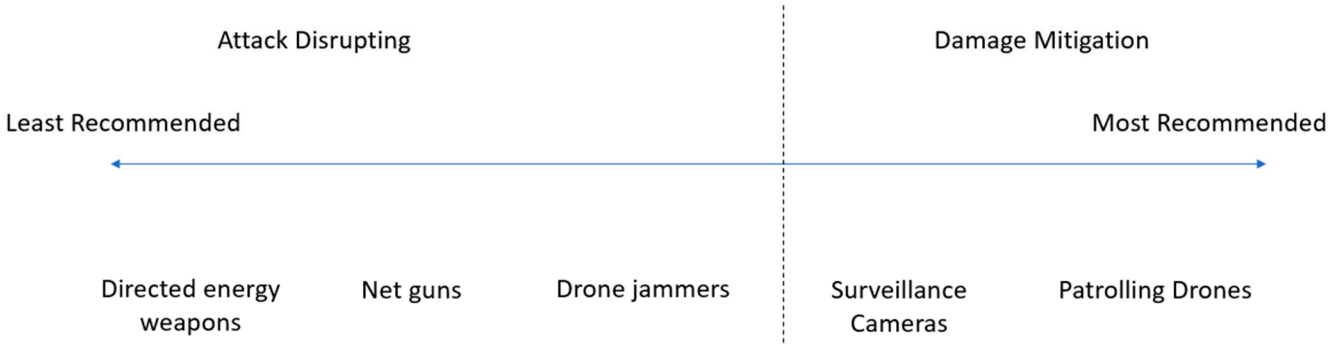

Figure 10. Recommendation of technologies based on technological maturity and complexity.

Table 3. Attack Disrupting (Physical vs. Not Physical).

Attack Disrupting	
Physical	**Not Physical**
• Net Gun • UAV guided nets	• Signal Jammers • Directed Energy Weapons

Table 4. Damage mitigation (Surveillance Cameras vs. Drones).

Damage Mitigation (Surveillance Cameras vs. Drones)	
Surveillance Cameras	**Patrolling Drones**
• Constant data from all points throughout the grid • High complexity with the number of cameras needed to cover the grid • Potential to be fully automated	• Data only while drones are up and from locations where they are located • Lower complexity due to the need for fewer drones to cover the same area • Potential to be fully automated

After considering these findings, future research should focus on collecting more quantitative data on the financial projections and technical aspects of the technologies involved. The main problem that can be identified with these conclusions is that there needs to be more detailed information collected on areas such as the costs of technology and the area of surveillance to make a more exact assessment of solutions to the consumer drone problem.

6. Conclusions

The rapid increase in the use of consumer drones has accelerated over the last decade [53]. Along with this increase, the risk of attacks using these drones has risen. The relative ease and low cost of obtaining a drone and using it to interfere with power grids makes an attack such as this much more attractive and possible. There has already been a documented attempt to threaten the grid with a drone, and drones are already used to disrupt operations at locations such as sporting venues and airports, so this threat is very much prevalent in our society. With the frequency of these events expected to rise, implementing measures such as the ones listed above to counter the effects of these attacks will significantly protect our critical national infrastructure from damage.

These measures can also be used to improve security on other hard-to-defend infrastructure such as rail lines and pipelines. Measures such as using drones to monitor the surroundings of the infrastructure for threats can have multiple uses while allowing the operators to identify and locate the problem faster. This will also advance the resilience of critical national infrastructure in the future. The nature of these attacks is their high impact and low frequency, so being able to return system operations to normal as fast as possible is a key benefit.

Another aspect to take into account with grids of the future are smart grid technologies. With the future of smart grid technology, the devices that are added and the data collected, such as cameras and video footage, can combat drones and serve various other purposes. The cameras and sensors to detect drones also have the potential to add to the overall maintenance and safety of the grid. The effects of natural disasters such as fallen trees and broken lines can be found because these methods all collect data on the physical condition of the distribution lines and the nearby areas. They can also reduce the costs of regular transmission line patrolling. Especially in cases where helicopters and a lot of human resources are needed to patrol a section of the line, cameras and drones can provide a low-cost and fast way of gathering information. While these technologies are analyzed as anti-drone methods, the other potential uses of these technologies cannot be overlooked because they also contribute to making the cost of implementation more feasible.

Finally, we need to prioritize the deployment locations as well as optimize the implementation of these anti-drone strategies. An investigation evaluating the importance of resiliency throughout the grid is needed to better determine what anti-drone measures should be used and where they should be taken. There also needs to be feasibility studies done on currently available measures to assess the economics of applying them. These two areas are the next steps that need to be carried out to further understand how to better defend the grid. It will be interesting to look out for future developments of anti-drone measures in other countries that are active in drone technologies such as China.

We plan to explore these recommendations to narrow the possible solutions and to identify parameters on their feasibility to limit the options. Currently, the topic and solutions are very broad, and more specifics need to be developed to come up with exact plans for implementation. Furthermore, given more recent events such as the recent attacks on power stations with firearms around the US [54], whether methods to prevent future attacks of that nature can be combined with drone defense should be seen.

Author Contributions: Conceptualization, A.K. and P.W.T.P.; methodology, A.K. and P.W.T.P.; formal analysis, A.K.; investigation, A.K.; resources, A.K., A.M. and P.W.T.P.; data curation, A.K.; writing—original draft preparation, A.K.; writing—review and editing, K.A., A.M. and P.W.T.P.; visualization, A.K.; supervision, A.M. and P.W.T.P.; project administration, P.W.T.P.; All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. America's Cyber Defense Agency. "Unmanned Aircraft Systems (Uas)—Critical Infrastructure". CISA. Available online: https://www.cisa.gov/uas-critical-infrastructure (accessed on 12 May 2022).
2. Lykou, G.; Moustakas, D.; Gritzalis, D. Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies. *Sensors* **2020**, *20*, 3537. [CrossRef] [PubMed]
3. Likely Drone Attack on Pennsylvania Substation. Smart Energy International. 2021. Available online: https://www.smart-energy.com/industry-sectors/energy-grid-management/likely-drone-attack-on-pennsylvania-substation/ (accessed on 10 May 2022).
4. DJI Mavic Air 2. Available online: https://www.bhphotovideo.com/c/product/1558184-REG/dji_cp_ma_00000176_03_mavic_air_2.html/?ap=y&smp=y&lsft=BI%3A6879&gclid=EAIaIQobChMI6d7MhpHt9gIVBsPVCh312AnHEAQYASABEgI2m_D_BwE (accessed on 19 May 2022).
5. Karanja, P. Guide to How Much Drones Cost. Droneblog. 2022. Available online: https://www.droneblog.com/drones-cost/ (accessed on 12 May 2022).
6. ABC News. WATCH: Intelligence Bulletin Reveals Plot against U.S. Electrical Grid Using Drone. Wjla. Available online: https://wjla.com/news/nation-world/watch-intelligence-bulletin-reveals-plot-against-pennsylvania-electrical-grid (accessed on 15 May 2022).
7. Nezamoddini, N.; Mousavian, S.; Erol-Kantarci, M. A risk optimization model for enhanced power grid resilience against physical attacks. *Electr. Power Syst. Res.* **2017**, *143*, 329–338. [CrossRef]
8. Wintch, T.M. PERSPECTIVE: Cyber and Physical Threats to the U.S. Power Grid and Keeping the Lights on. Hstoday. Available online: https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/ (accessed on 16 May 2022).
9. Barrett, B. A Drone Tried to Disrupt the Power Grid. It Won't Be the Last. *Wired*, 5 November 2021. Available online: https://www.wired.com/story/drone-attack-power-substation-threat/(accessed on 20 May 2022).
10. Critical Infrastructure Sectors. CISA. Available online: https://www.cisa.gov/critical-infrastructure-sectors (accessed on 23 May 2022).
11. Marcy, C. EIA Study Examines the Role of High-Voltage Power Lines in Integrating Renewables. EIA. Available online: https://www.solarpowerworldonline.com/2018/07/eia-study-examines-the-role-of-high-voltage-power-lines-in-integrating-renewables/ (accessed on 1 June 2022).
12. Kayastha, N.; Niyato, D.; Hossain, E.; Han, Z. Smart grid sensor data collection, communication, and networking: A tutorial. *Wirel. Commun. Mob. Comput.* **2014**, *14*, 1055–1087. [CrossRef]
13. TSA Begins Testing Drone Detection Technology at LAX. TSA. Available online: https://www.tsa.gov/news/press/releases/2022/08/25/tsa-begins-testing-drone-detection-technology-lax (accessed on 1 June 2022).
14. Paramanik, S.; Sarkar, P.S.; Mondol, K.K.; Chakraborty, A.; Chakraborty, S.; Sarker, K. Survey of Smart Grid Network Using Drone & PTZ Camera. In Proceedings of the 2019 Devices for Integrated Circuit (DevIC), Kalyani, India, 23–24 March 2019; pp. 361–364. [CrossRef]
15. Vargas, M.; Vivas, C.; Rubio, F.R.; Ortega, M.G. Flying Chameleons: A New Concept for Minimum-Deployment, Multiple-Target Tracking Drones. *Sensors* **2022**, *22*, 2359. [CrossRef] [PubMed]
16. Electricity Grid Resilience: Climate Change Is Expected to Have Far-reaching Effects and DOE and FERC Should Take Actions. 2021. Available online: https://www.gao.gov/assets/gao-21-423t.pdf (accessed on 15 May 2022).
17. Sultan, V.; Hilton, B. Electric grid reliability research. *Energy Inform.* **2019**, *2*, 3. [CrossRef]
18. Rothe, J.; Strohmeier, M.; Montenegro, S. A concept for catching drones with a net carried by cooperative UAVs. In Proceedings of the 2019 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR), Würzburg, Germany, 2–4 September 2019; pp. 126–132.
19. Multerer, T.; Ganis, A.; Prechtel, U.; Miralles, E.; Meusling, A.; Mietzner, J.; Ziegler, V. Low-cost jamming system against small drones using a 3D MIMO radar based tracking. In Proceedings of the 2017 European Radar Conference (EURAD), Nuremberg, Germany, 11–13 October 2017; pp. 299–302.
20. Souli, N.; Kolios, P.; Ellinas, G. Multi-Agent System for Rogue Drone Interception. *IEEE Robot. Autom. Lett.* **2023**, *8*, 2221–2228. [CrossRef]

21. Chary, S.U.M.; Sekhar, B.P.C. Design and Optimization OF Drone Jammer Antenna Using Structural Analysis. *arXiv* **2022**, arXiv:2202.00973.
22. Tyler, N. Gatwick Game-Changer. *New Electron.* **2019**, *52*, 16–18. [CrossRef]
23. Northfield, R. Throw away the key: Doing time with technology. *Eng. Technol.* **2018**, *13*, 34–38. [CrossRef]
24. SkyFence. Available online: https://www.dronedefence.co.uk/skyfence/ (accessed on 22 April 2022).
25. UAV Jammer Drone Blocker Protect You From Sneak Shots By Drones. Dojammer. Available online: https://www.dojammer.com/uav-drone-blockers.html#:~:text=Drone%20jammers%20can%20display%20jamming,range%20can%20reach%202%20kilometers (accessed on 13 May 2022).
26. Matić, V.; Kosjer, V.; Lebl, A.; Pavić, B.; Radivojević, J. Methods for Drone Detection and Jamming. In Proceedings of the 10th International Conference on Information Society and Technology (ICIST), Kopaonik, Serbia, 8–11 March 2020; pp. 16–21.
27. Paladyne E2000HH. Dronedefence. Available online: https://www.dronedefence.co.uk/paladyne-e2000hh/ (accessed on 15 May 2022).
28. Directed Energy. Available online: https://www.lockheedmartin.com/en-us/capabilities/directed-energy.html (accessed on 15 May 2022).
29. "Trey" Obering, H., III Directed Energy Weapons Are Real ... And Disruptive. *PRISM* **2020**, *8*. Available online: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Obering_36-46.pdf (accessed on 3 June 2022).
30. Coffey, V.C. High-Energy Lasers: New Advances in Defense Applications. *Opt. Photonics News* **2014**, *25*, 28–35. [CrossRef]
31. Available online: https://www.boeing.com/defense/missile-defense/directed-energy/index.page (accessed on 12 May 2022).
32. Grose, T.K. Drone Killer. *ASEE Prism* **2019**, *29*, 13.
33. High Energy Lasers. Available online: https://www.raytheonintelligenceandspace.com/what-we-do/advanced-tech/lasers#:~:text=This%20directed%20energy%20technology%20enables,%2C%20rockets%2C%20artillery%20and%20mortars (accessed on 12 May 2022).
34. Keeping UAVs away from the Game. Raytheon Intelligence and Space. Available online: https://www.raytheonintelligenceandspace.com/news/2021/05/05/keeping-uavs-away-game (accessed on 23 April 2022).
35. Associated Press. Beam It Right There, Scotty. *Wired*, 10 July 2005. Available online: https://www.wired.com/2005/07/beam-it-right-there-scotty/#:~:text=The%20hallmark%20of%20all%20directed,frequencies%2C%20it%20can%20penetrate%20walls(accessed on 14 May 2022).
36. OphirBlog. Directed-Energy Laser Devices—Advantages and Challenges. 2021. Available online: https://blog.ophiropt.com/directed-energy-laser-devices-advantages-and-challenges/ (accessed on 2 May 2022).
37. Weinberg, G.V. Performance prediction of directed energy weapons. *Prog. Electromagn. Res. M* **2022**, *108*, 79–88. [CrossRef]
38. Laser Directed Energy Weapons Likely to Receive the Most Investment in Future: Poll. Available online: https://www.airforce-technology.com/news/laser-directed-energy-weapons-likely-to-receive-the-most-investment-in-future-poll/ (accessed on 15 May 2022).
39. Schaub, D.M.W.H. Six Ways to Disable a Drone. Available online: https://brookings.edu/blog/techtank/2016/03/16/six-ways-to-disable-a-drone/ (accessed on 15 May 2022).
40. Available online: https://netgun.com/netgun-info/ultranet-small-animal-netgun (accessed on 27 May 2022).
41. Pledger, T. The Role of Drones in Future Terrorist Attacks. *Assoc. United States Army* **2021**, *137*, 26.
42. Gacek, J. Species justice for police eagles: Analyzing the Dutch "flying squad" and animal-human relations. *Contemp. Justice Rev.* **2018**, *21*, 2–16. [CrossRef]
43. Mizokami, K. The U.S. Army Plans To Field the Most Powerful Laser Weapon Yet. *Pop. Mech.* **2019**. Available online: https://www.popularmechanics.com/military/weapons/a28636854/powerful-laser-weapon/ (accessed on 19 May 2022).
44. Iversen, N.; Schofield, O.B.; Cousin, L.; Ayoub, N.; Vom Bögel, G.; Ebeid, E. Design, integration and implementation of an intelligent and self-recharging drone system for autonomous power line inspection. In Proceedings of the 2021 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Prague, Czech Republic, 27 September–1 October 2021; pp. 4168–4175.
45. Sciences, A.F. Aurora Tests Improved MIDAS Counter-UAS System. Available online: https://www.aurora.aero/2022/04/25/aurora-tests-improved-midas-counter-uas-system/ (accessed on 21 May 2022).
46. Bruns, I. Drones for Power Line Inspections—Utility Products. Utility Products. Available online: https://www.utilityproducts.com/line-construction-maintenance/article/16003823/drones-for-power-line-inspections (accessed on 15 May 2022).
47. Nichols, G. Cheap GPS Jammers a Major Threat to Drones. Zdnet. Available online: https://www.zdnet.com/article/cheap-gps-jammers-endanger-drones/#:~:text=Today%2C%20jammers%20can%20be%20bought%20online%20for%20as%20low%20as%20%2450 (accessed on 15 May 2022).
48. Chiper, F.-L.; Martian, A.; Vladeanu, C.; Marghescu, I.; Craciunescu, R.; Fratu, O. Drone detection and defense systems: Survey and a software-defined radio-based solution. *Sensors* **2022**, *22*, 1453. [CrossRef] [PubMed]
49. How Much Does a Commercial Video Surveillance System Cost? Costowl. Available online: https://www.costowl.com/b2b/security/security-video-surveillance-commercial/#:~:text=Generally%2C%20you%20can%20expect%20to,a%20camera%20is%20not%20enough (accessed on 20 May 2022).

50. Vugrin, E.D.; Castillo, A.R.; Silva-Monroy, C.A. *Resilience Metrics for the Electric Power System: A Performance-Based Approach*; Sandia National Lab.(SNL-NM): Albuquerque, NM, USA, 2017. Available online: https://www.osti.gov/biblio/1367499 (accessed on 15 May 2022).
51. Chen, H.; Egan, D.M.; Seiler, K.; Bryson, M.E.; Bresler, F.S., III. PJM: Probabilistic Risk Assessment for Spare Transformer Planning. In *Power System Assets: Investment, Management, Methods and Practices*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 415–428.
52. Siahaan, Z.A.; Wijaya, A.; Chandra, J.A.; Banjar-Nahor, K.M.; Hariyanto, N. Fault Current Limitation Roadmap to Anticipate the Problem of High Fault Currents in Indonesian Java-Bali Power System. In Proceedings of the 2022 IEEE International Conference on Power Systems Technology (POWERCON), Kuala Lumpur, Malaysia, 12–14 September 2022; pp. 1–6. [CrossRef]
53. Drones by the Numbers. Available online: https://www.faa.gov/uas/resources/by_the_numbers/ (accessed on 20 May 2022).
54. Two Charged with Attacks on Four Pierce County Power Substations. DOJ. 2023. Available online: https://www.justice.gov/usao-wdwa/pr/two-charged-attacks-four-pierce-county-power-substations (accessed on 20 May 2022).