Intellectual Property & Cybersecurity in Additive Manufacturing within the Defense Sector

A new capability enhancing cybersecurity and readiness at the speed of relevance.

DEFENDED

Microsoft Azure

Digital platforms in all areas of the economy are targets for cybercrime and IP theft.

Industry 4.0 is no different, it represents a prime target for adversaries.

DEFEND3D is introducing new patented technology in this paper to combat that threat, centered around secured ownership and complete retention of IP. The IP (Digital file) no longer needs to be shared with internal or external clients or manufacturers.

DEFEND3D is the leading manufacturing solution enabling secure transmission for remote 3D printing with its One-Click-Print capability using VICI: Virtual Inventory Communications Interface.

Author

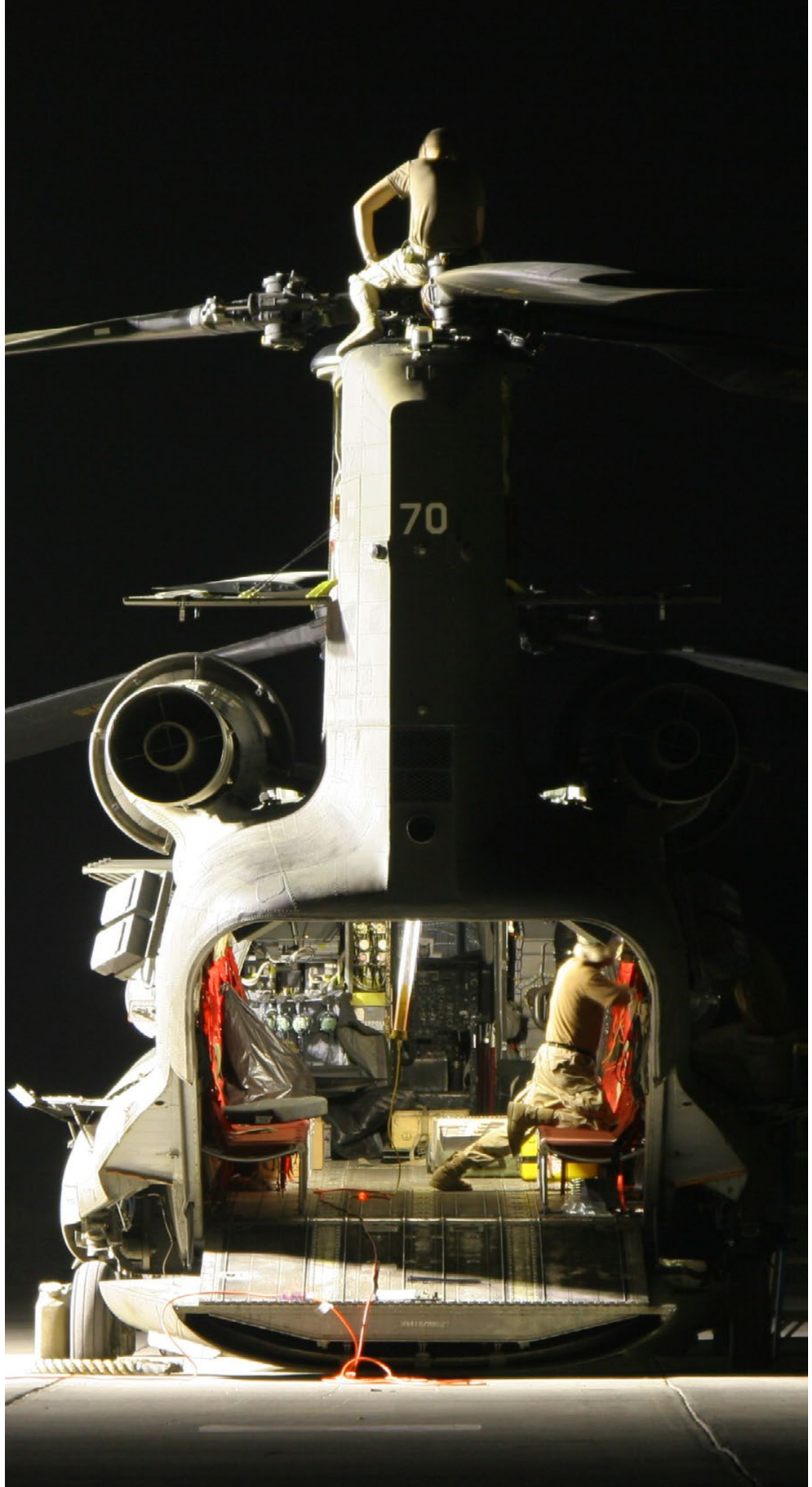
Walter Veldsman is the Director of the engineering consultancy, IGWC UK Ltd. He is a Chartered Professional Engineer with over 30 years' experience in a variety of sectors including Oil & Gas, Nuclear, Aerospace, Automotive and General Engineering, both nationally and internationally.

He has managed product development for the BOC Group / Linde Group developing a range of new products which were successfully launched into the marketplace. He has provided technical expertise and direction in product development across the globe, winning the best Research and Development Engineering Project award in the UK. With over 15 years' experience in the role of Global Technical Manager he has a thorough understanding of the diverse engineering challenges across the world.

Veldsman is a visionary and innovator, committed to continuous improvement. This is evidenced by him being granted six patents, four of which cover the Additive Manufacturing engineering field. Veldsman has published many papers at national and international conferences.

Walter Veldsman
CEng. MSc(Eng.)

IGWC Ltd



Co-Author

Walid is leading AI and Sustainability in manufacturing and energy at Microsoft in the USA. His team drives Industry 4.0 and cutting-edge technology deployments and is excited to both lead the disruptive technology innovation while also skilling the workforce for the ever changing workforce transformation.

Before joining Microsoft, he led the Google cloud worldwide edge and distributed artificial intelligence solutions. Prior to joining Google, Walid was the chief technologist at AMD edge and cloud group. He was also Intel's global cloud solutions team manager, revolutionizing AI in the line of business at major international banks, exchanges, media, cloud and Telco's customers.

Walid holds 57 granted patents with the USA patent office and more than 40 peer-reviewed technical publications and key AI conferences. Walid has studied executive management at Harvard business school and holds a PhD in Electrical and Computer Engineering from Drexel University, Philadelphia. He received his MSc in Computer Science from Imperial College London, UK with distinction.

Walid Ali
Artifical Intelligence at Microsoft

Microsoft Azure

Contents

11 **Executive Summary**

12 **Chapter 1.0 Introduction**

16 **Chapter 2.0 AM in Defense**

16 2.1 AM Developments in Defense

22 2.2 Mobile AM Hubs on Site in Theatres of War

24 **Chapter 3.0 Literature Review**

24 3.1 The IP Cybercrime & IP Protection Problem

30 3.2 Cybercrime & IP Theft Costs to Industry

31 3.3 General Overview of Cybercrime in AM

40 **Chapter 4.0 MOD Case Study**

40 4.1 DEFEND3D - A New Patented Solution

42 4.2 Testing & Performance Requirements

45 4.3 Summary of Results

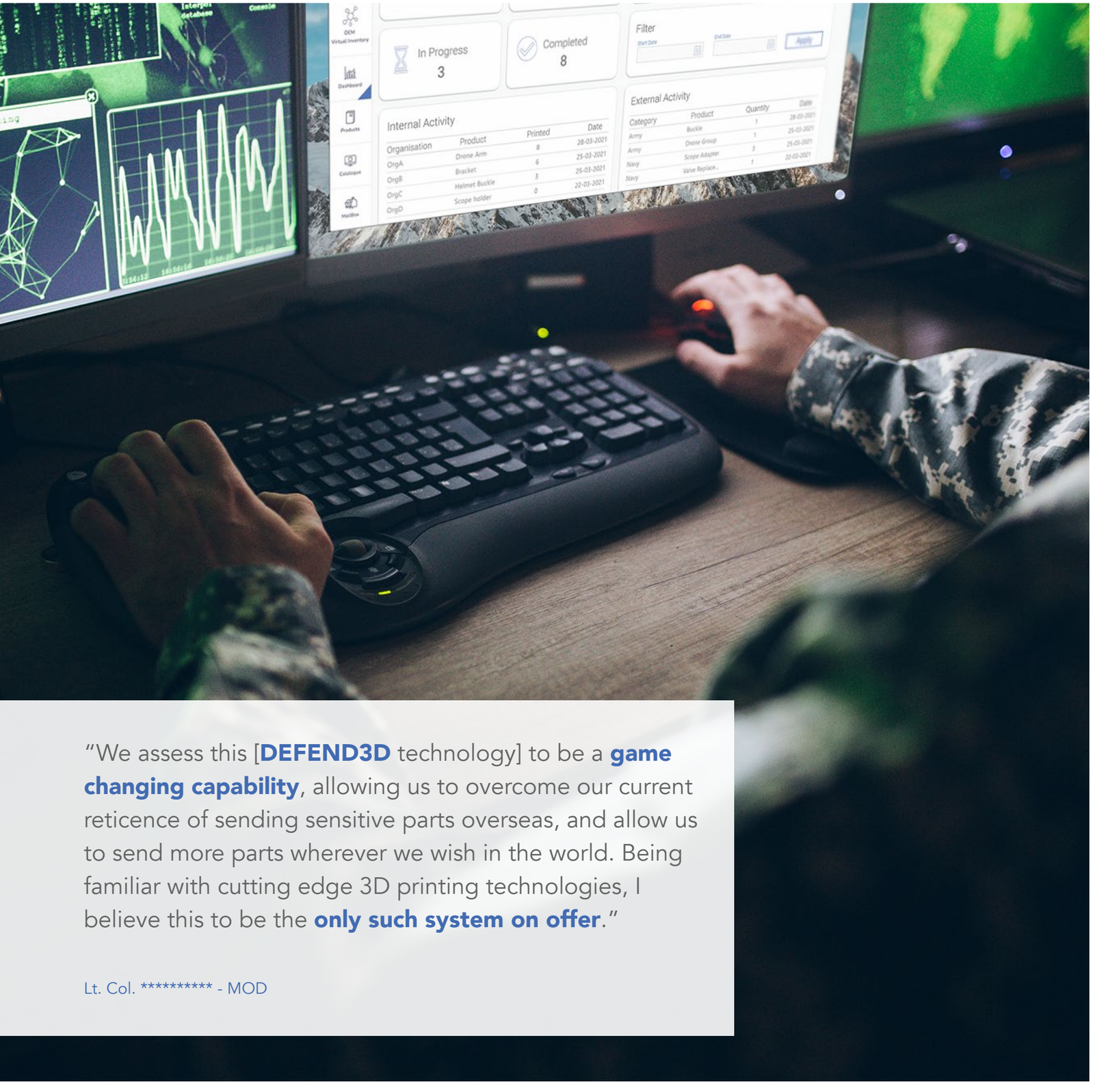
46 **Chapter 5.0 Discussion**

50 **Chapter 6.0 Conclusion**

54 **Bibliography**

58 **List of Figures**

59 **Glossary**



"We assess this [**DEFEND3D** technology] to be a **game changing capability**, allowing us to overcome our current reticence of sending sensitive parts overseas, and allow us to send more parts wherever we wish in the world. Being familiar with cutting edge 3D printing technologies, I believe this to be the **only such system on offer**."

Lt. Col. ********** - MOD

Executive Summary

In order to execute core missions domestically and abroad, Defense organizations must be able to sustain their forces in a responsive and cost-effective manner. Any tactical advantage can prove decisive in an engagement. Having a secure Additive Manufacturing digital supply thread and printing facility in a theatre of war is one such advantage in terms of sustainment, improved operational readiness and higher sortie rates.

This paper addresses Additive Manufacturing's perennial problem of IP and cybersecurity within the Defense sector. Currently the entire digital file is transferred to the fabrication machine, making the digital IP vulnerable to cyberattacks, manipulation and theft. Various solutions have been proposed to try and solve the issue of IP exposure so that warfighters have access to critical parts on demand, including blockchain, encryption and licensing business models. However, all of these solutions still require that the entire digital file is transferred.

DEFEND3D is a new and patented technology for the transmission of remote 3D printing, CNC machining, laser cutting, Bioprinting and other digital manufacturing data with One-Click-Print. This game changing cybersecurity and transmission protocol enables a secure digital resupply of reproduction parts to remote locations without the necessity of any file transfer. DEFEND3D has been successfully tested by UK Strategic Command, a division of the UK Ministry of Defence (MOD), where provision of a Secure Platform for Digital Manufacturing has been delivered.

Manufacturing standards and part integrity is key. Benchmark testing with the MOD shows that printing time and quality is not affected when using the DEFEND3D transmission service, even when compared to the print of an SD card and at a low bandwidth of 56 Kbps and at a high latency of a round trip greater than 3000 miles.

Chapter 1.0
Introduction

Cybercrime and specifically Intellectual Property (IP) security is a major problem in the Additive Manufacturing (AM) industry. [1,2,3] This paper overviews the current situation, the nature of the problem, issues and consequences faced by IP owners.

The importance, significance and impact of the cybercrime problem will be determined by the market segment associated with it.

Defense
A cyberattack on a 3D printing facility supporting military activity in a theatre of war has the potential to negatively impact the outcome of the engagement.

General Manufacturing
Many AM companies in this sector are grappling with the cybersecurity challenges in front of them. The exposure extends to multiple node vulnerabilities in the full digital thread or chain.[4] Partial solutions are available that may not fully protect the multiple vulnerable nodes of the digital thread, thus exposure might be reduced but not eliminated.[5]

Biological Additive Manufacturing (Bio AM)
There is considerable competition in 3D Bioprinting around the world. Many countries and institutions are funding intensive research in this area where significant breakthroughs have already been made.

Campobasso[6] states "If the U.S. successfully implements a Bioprinting enhancement program, it is likely that other countries would be very interested in acquiring similar technology and may try to steal information associated with the program. Because part of the Bioprinting process is electronic, would it be vulnerable to cyber hacking or theft? As 3D Printers become more accessible, could non-state actors steal digital blueprint information and replicate U.S. Bioprinted enhancements on their own?

"We believe this program has **the potential to reduce logistical challenges** and costs for transporting medical supplies to austere environments, which could also be applied to our special operations forces in remote locations. **Instead of carrying tons of supplies, they could just print them**"

Dr. Vincent Ho, Director of USU's 4D Bio3

Figure 1. (Above and Below) 3D Printing in a desert deployment zone [7]

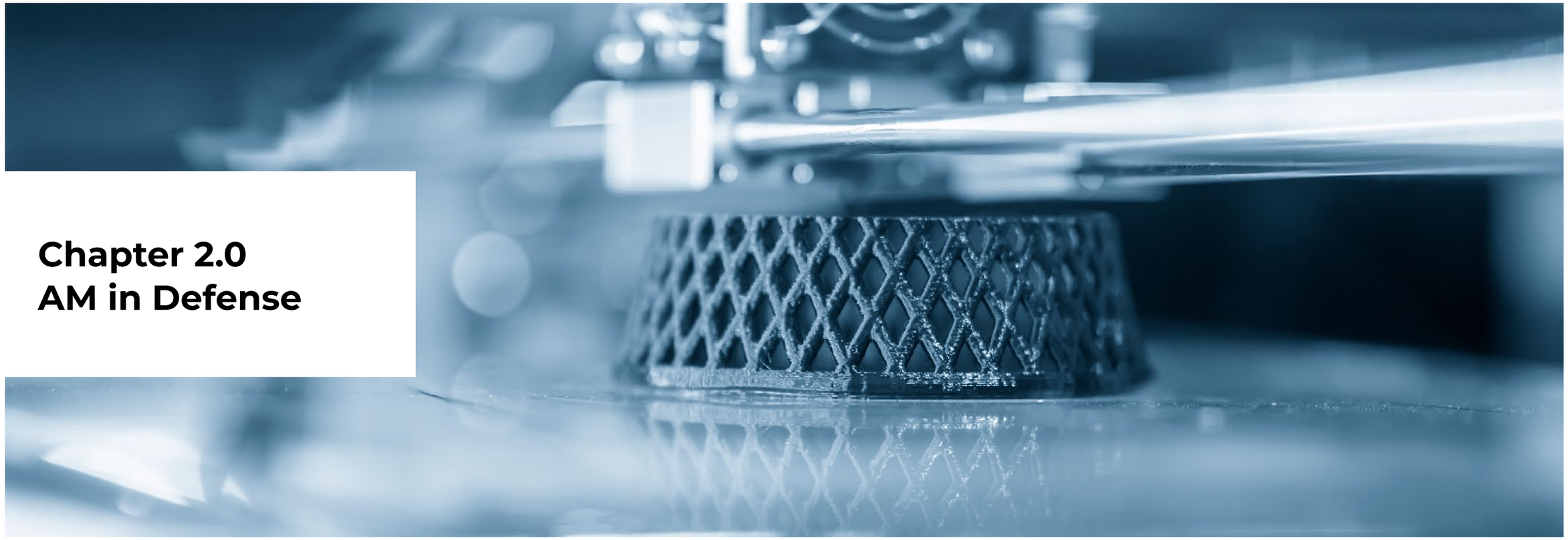
If the digital aspect of the program could be encrypted or electronically protected against foreign exploitation, it could prevent other countries or non-state groups from developing the same capabilities and negating the advantage that enhancements provide to the U.S. military".

Many papers have been published which characterize the nature of intellectual property protection in AM. A recent pilot program conducted by the Uniformed Services University of the Health Sciences in collaboration with the U.S. Military Academy has shown that a 3D Printer capable of Biofabrication could expedite, repair or perhaps replace damaged tissues for troops injured on the battlefield. This advancement could potentially change the way care is provided to the nation's deployed warfighters.

The use of 3D Printers in a forward-deployed desert environment (where resources may be limited) could massively improve logistical challenges and costs for transporting medical supplies to austere environments.

The ruggedized 3D Printer was sent to an undisclosed desert location with basic supplies and human mesenchymal stem/stromal cells (hMSCs), the only cells that allow for same day Bioprinting. [7]

On site, the 3D Printer was able to successfully fabricate a number of products, including surgical tools, Bioactive bandages and surgical models based on CT scan data. The image used to print was sent as an electronic file from a stateside facility to the remote environment, and printed on location – the first demonstration of cyber manufacturing where complex designs were transmitted and produced in a remote location.



Chapter 2.0
AM in Defense

2.1 AM Developments in Defense

The defense industry has recognized the potential of AM to make a strategic difference in a theatre of war which can give a combatant a significant agile advantage in terms of sustainment, improved operational readiness and higher sortie rates over a hostile adversary.

The US Army Secretary places 3D printing at the center of modern defense policy.[8] Many defense organizations like the US Department of the Navy (DON) have published their 'Additive Manufacturing Implementation Plans' as a commitment to moving into advanced and additive manufacturing.[9]

Many defense organizations in countries around the world have invested heavily in AM, so much so that the results of these investments are starting to show with regards to the final products of their research in defense applications.

A host of papers have been published showing a multitude of AM products for applications across the whole defense sector including the Army, Navy, Air Force and Space.

2.1.1 Case Study Examples

Osprey VTOL with 3D Printed Parts [11]
Osprey VTOL aircraft make use of a 3D printed titanium link fitted inside the engine's nacelle. The Navy's years of experience in 3D printing and AM have enabled them to develop and print flight critical components.

Utilizing technologies such as Microsoft Machine Learning (ML) and Intelligence at the Edge solutions,

We live in an era of extraordinary technological change and **we must make sure we are harnessing the power of innovation** by working as efficiently and effectively with industry as possible".[10]

UK Defence Secretary Ben Wallace

"**3D Printing** is about to **save** the military **billions of dollars**."

Will Roper, Former Assistant Secretary of the Air Force (Acquisition)

3D printing flight critical components becomes more secure, flexible and faster. Additional 3D printing options could innovate the operational excellence on ground from generating unstructured 2D data to 3D shapes via Inverse Graphics GAN.

Digital Twins, Legacy Parts [12]

There are serious challenges in the supply chain with regards to the purchasing of critical legacy parts on indispensable military assets that the US depends on for the nation's defense.

Examples of which include the C-5 Supergalaxy cargo plane, the KC-135 aerial re-fueler, the B-52 Bomber and the Black Hawk UH-60 alongside many other old military assets.

The supply chain problem relates to the age of the asset, the availability of drawings, the fleet size and the complexity of predicting the maintenance requirements and critical spare parts needed at any time. The specific problem in the legacy parts supply chain is that of supply (none) and demand (very infrequent and low volume).

This drives the cost equation dramatically for the military. The need to have critical legacy military assets available 24/7 in a war ready status (sustainment) accounts for about 70% of the total weapon's costs.

Manufacturers will not bid on low volume legacy parts due to the fact that they would need to convert old 2D drawings to 3D designs then check they meet all the latest modern regulatory standards then dedicate equipment and a team of specialists for a small production that may never repeat.

The military must then raise the offering price to encourage a manufacturer to bid.

Will Roper, former Assistant Secretary of the Air Force for acquisition says that an example of this is a C-5 aft pressure door handle that cost $2,800 in 2018 because manufacturers would not bid when the price was lower.

The Black Hawk UH-60 is a case in point and like other aerospace projects it faces issues with the legacy part supply chain. The Black Hawk helicopter entered Army service in 1979. As such, some of the components are at least 40 years old. Wichita State University's National Institute for Aviation Research (NIAR) will create a Digital Twin of the said Black Hawk helicopter with the goal of developing a 3D printing parts replacement assembly line. A solution is in sight in the form of The Digital Twin.

The engineers at NIAR are building the Digital Twin with the explicit intention of creating legacy hardware to be 3D printed.

To tackle serious challenges in the supply chain for the purchasing of critical legacy parts on indispensable military assets, multiple Microsoft services can be leveraged. Azure Digital Twins can be utilized for simulating spare parts design, production and supply chain processes in conjunction with Azure ML services.

As well as this, Azure IoT services can be used for securing, monitoring and forecasting legacy parts production processes as well as exchanging production and delivery data with supplier and other stakeholders via Cloud-based Manufacturing Intelligence.

F-22 Raptor Fighter Aircraft with Metallic 3D Printed Parts [13]

The US Air Force F-22 Raptor fighter aircraft manufactured by Lockheed Martin and Boeing has its first titanium 3D printed metal part installed.

Figure 2. 3D Printed Grenade Launcher [18]

> "Rather than run a supply requisition all the way back to a depot, maybe we just print parts on the spot. At this time of great challenge, I see great opportunity. **Can we think of leap-ahead ways to do supply differently?**"
>
> Dr Mark T. Esper - Secretary of the Army 2018

Due to the supply chain challenges associated with small fleet sizes and replacement parts, it has become necessary to use on-demand 3D printing capabilities to solve this problem. The solution enabled a faster and more cost efficient replacement of a damaged part with a 3D printed solution, substantially reducing downtime of the aircraft. The titanium brackets are expected to last longer due to its higher corrosion resistance and shorter lead-time, providing increased aircraft readiness.

The Air Force has plans to incorporate at least five more metallic AM parts in the F-22, resulting in a significant reduction in maintenance down-time.

The Military Have Intentions of 3D Printing Drones [14,15]

The military are increasingly using 3D additive manufactured drones to give them intelligence capability over horizons that only a drone could deliver. This capability is now a reality in war zones. Having the 3D additive capability in a war zone can deliver a decisive advantage for a combatant with specific regards to manufacturing or repairing drones on site.

This more cost-efficient and precise method can be achieved by utilizing Azure IoT Hub (Cloud-based Manufacturing Intelligence) for prediction functions and 3D printing process security. In addition to this, Microsoft AI AirSim drones and AI self-aware drones help to create simulated 3D images of the environment and process the custom vision model.

Combined with the ability to manufacture and repair drones on site, drone application costs can be lowered while the flexibility of combat drones are increased.

British Army to Use 3D Printed High Explosives [16]

The Defence Science and Technology Laboratory (DSTL) has funded a research program to study and design optimized 3D printed explosives for use in theatres of war.

The MOD has invested £10 million to create new innovative and efficient explosives for use in unique and niche applications while delivering lower transportation and storage costs.

Serverless Cloud Computing and AI Powered Mappings on Microsoft Azure ML platform, combined with SDK for Python and Field Programmable Gate Array (FPGA) means the Microsoft platform benefits by accelerating learning for research programs. This can aid in study and design to optimize 3D printed explosives with seamless interoperability of proprietary IT-systems and newest data modelling for machine learning. High-Performance Computation on Azure enables faster results of high complex simulations and workloads.

3D Printed Parts for Tanks [17]

The U.S. Marine Corps has plans to use 3D printed impellers on M1A1 Abrams main battle tanks after successful field trials when the original parts wear or become inoperable and no spare replacement part is immediately available.

3D Printed Grenade and Grenade Launcher [18]

Researchers at the U.S. Army Armament Research, Development and Engineering Center (ARDEC) successfully fired a 3D printed grenade from a 3D printed grenade launcher. This gives the military a future weapons development capability with the use of 3D Additive Manufacturing. One can expect all kinds of innovative developments in this area driven by the need for engineers to provide munitions to soldiers more quickly.

"It is my strong belief that **3D printing and advanced manufacturing are breakthrough technologies** for our maintenance and logistics functions in the future."[19]

Vice Admiral Philip Cullom United States Navy

One option would be to use IoT services by Microsoft Azure to 3D print parts for military vehicles or weaponry via seamless Robotic Control and Edge Computing for offline applications.

2.2 Mobile AM Hubs on Site in Theatres of War

Mobile AM hubs are being incorporated in the military's arsenal of manufacturing and maintenance facilities in theatres of war. This is to attain maximum combative capacity, readiness and agility to facilitate optimum operational readiness for engagements and sorties.

By incorporating Digital Twins, Edge Computing in combination of IoT Device Simulations and cloud operation via IaaS/PaaS will streamline every manufacturing and maintenance operation inside and across any facility. Special high sensitive production operations may be secured via a VPN of VM instances. All digital process can be visualized and made easily reportable via Power BI.

Dutch Navy's Mobile AM Hub [20]
When on mission, the Dutch Navy must carry up to 30,000 spare parts on board, ranging from critical spares for engines to relatively minor parts.

Predicting which spares may be required for equipment is very complex. They cannot rely on its supply chain in a theatre of war as lead times may be impractically long.

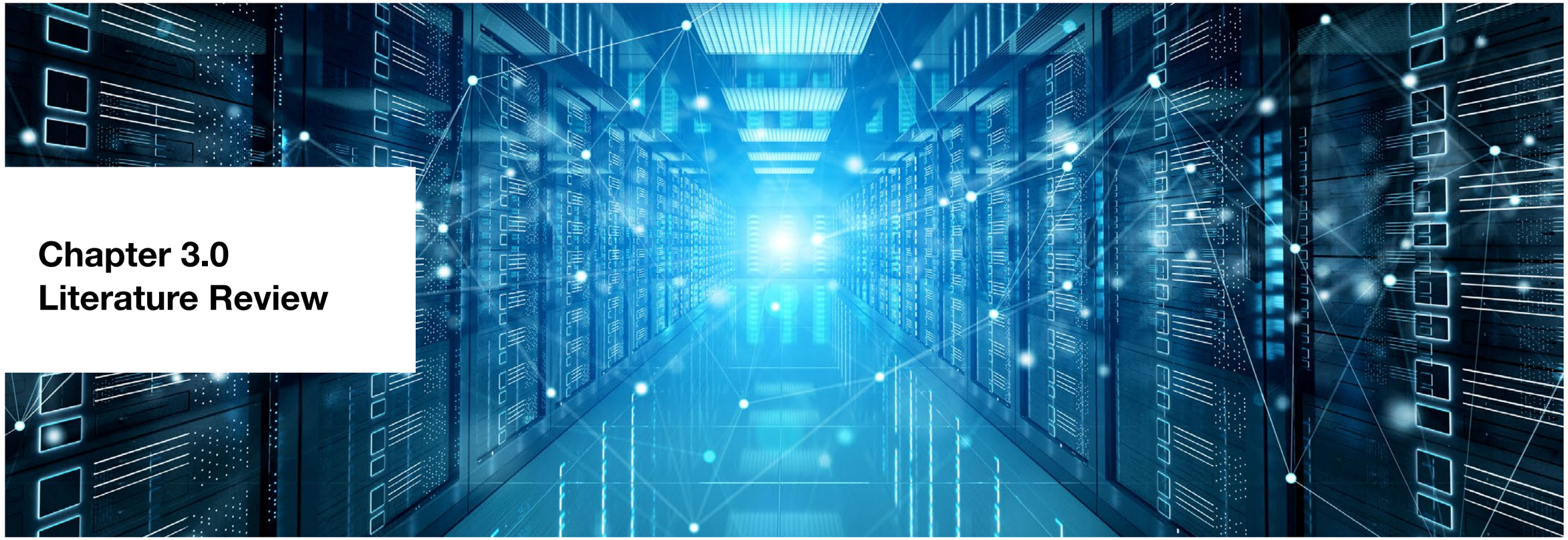
This has caused the Dutch Navy to invest in AM to reduce its dependence on its current supply chain so that spares can be printed on demand. They believe it can reduce their carrying and storage of spare parts as well as increase its operational deployment significantly.

Azure ML for Predictive Maintenance helps forecast which spares will be required for equipment. This complex process of inventory monitoring can be eased by incorporating Edge Computing for Inventory of spare parts. A Virtual Network on VM instances for highly sensitive inventory data sharing, can be used if needed.

Mobile AM Hub for the United States Department of Defense (DoD) [21]
The US Department of Defense has invested in the manufacture of a fully operational and capable mobile AM Hub contained in a standard shipping container which can be deployed immediately into the field via land, air or sea.

ExOne is developing a special military-edition 3D printer that can binder jet 3D print more than 20 metal, ceramic, and other powder materials into direct final products or tooling.

Operationalizing the full Azure Stack Service for mobile AM hub containers enables easy setup, operations, security and monitoring of each AM container and the whole container fleet. Adding Serverless Computing increases off-site manufacturing, VPN Gateways and Private Networks stabilize secure communication if needed.



Chapter 3.0
Literature Review

3.1 The IP Cybercrime & IP Protection Problem

The nature of the cyberattacks on vulnerabilities in the Digital Thread of the AM industry include:

- Technical Data Theft
- Industrial Espionage
- Intellectual Property Theft
- Counterfeiting
- Reverse Engineering
- AM Sabotage
- Manipulations

All of the above threats can have serious implications for Defense organizations.

3.1.1 Technical Data Theft

AM build files are prime targets for theft as they contain the full CAD 3D design detail and the full G-code instructions which are needed by the AM machine controller to manufacture the component.

An option could be the operationalizing of the full Azure Stack Service in combination with VPN gateways, VM storage and VM Computation. This architecture can be used for the establishment of anti-cybercrime and IP protection for any 3D printing use case in manufacturing. The 3D designs are often a result of refined topological optimization known as Finite Element Analysis (FEA) which results in optimized mechanical and product performance (i.e. fracture and fatigue).

ML and high performance computation enable faster topological optimization, stress engineering and simulations of mechanical and product performance. Simulation of operational fracture and fatigue risks can be identified more quickly and at a lower cost.

Gaining access to these files bypasses the associated costs and time involved in the research and development of a product.

3.1.2 Industrial Espionage

Industrial espionage (otherwise known as economic espionage, corporate spying or corporate espionage) is a form of espionage conducted for commercial purposes between companies or corporations often seeking to gain access to their competitor's latest technology or products.

Whilst theft is more common to developing economies, developed economies are more likely to encounter hostile industrial espionage that focuses on high value industries such as space and military. The implications of this may adversely affect the country as a whole.

Using IaaS by Microsoft combined with Azure services and Azure Data Share (which feature end-to-end traceable data access logs) ensure high level control of IP/data access and set high security standards against industrial espionage.

3.1.3 Intellectual Property Theft

IP infringement can occur if an intellectual property right is violated. There are several types of intellectual property rights, such as copyrights, patents, trademarks, industrial designs and trade secrets. The legal definitions and scope will change from country to country.

Roughly **400 Manufacturers** were attacked everyday during 2016, amounting to about **$3 billion** in combined **losses**.

National Defense NDIA's Business and Technology Magazine

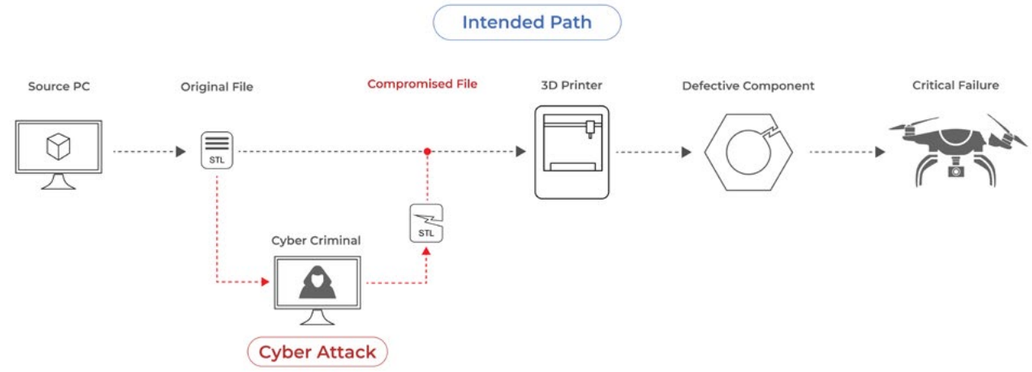


Figure 3. The impact of induced defects in critical components in the "dr0wned study" [22]

IP infringement may occur if one of the following is compromised:

- Copyright Infringement (e.g. illegally obtained design files)
- Patent infringement
- Design infringement

Critical IP theft can be an easy target for industrial competitors and rogue nations. Once stolen, the files can be copied without any restrictions and limits and there will be no limit to the number of components that can be manufactured or produced from that single stolen file. Alternatively, these files can be made available to others who would have the same illegal privileges. IaaS combined with Azure services such as Azure Stack, VM storage and data/file processing (paired with VPN Gateways) are one of the most secured IT-infrastructure components for securing IP from inside and outside risk factors.

Microsoft Insider Risk Management helps to quickly identify, detect, and act on insider threats. This solution leverages the Microsoft Graph and security services to analyze real-time native signals such as file activity, communications sentiment and abnormal user behavior.

3.1.4 Counterfeiting

AM build files contain both the AM 3D design IP and the complete instructions for the machine build. If these files are compromised or stolen, it is very easy to replicate the original item at the same build quality and achieve the same product performance levels, all without the research and development and the associated design costs.

This is a very attractive financial proposition for the counterfeiters. Theft is often perpetrated in the developing economies where labor and machine time is relatively cheap. Often the products might be sold locally where the theft would never be detected and its consequences never felt.

The original equipment manufacturers (OEMs) generally suffer the consequences one way or the other by means of a loss of potential market share or potential sales revenues. There are huge safety risks associated with counterfeit products entering the supply chain. Failure of these products could have serious consequences as well as affecting the brand equity of the original OEM's product.

For example, the Microsoft Deepfake Detector Tool can be applied for early detection of counterfeit products at supply chain gates.

3.1.5 Reverse Engineering

Physical products can be 3D scanned to recreate the 3D digital design if the original design files cannot be stolen.

The availability of cheap sophisticated 3D scanning systems in the market today accentuates this problem. Because of this, how can companies protect their IP? The level of reverse engineering can only increase with time as these systems are very popular in the market and are selling very well.

The current intellectual property laws and legal position is an evolving one. The developments in digital scanning outpaces the legal progress in this regard so that they are always a step behind the technological developments, always playing catch up.

In future, intellectual property laws will be decided by case law in country courts of law. More clarity on the

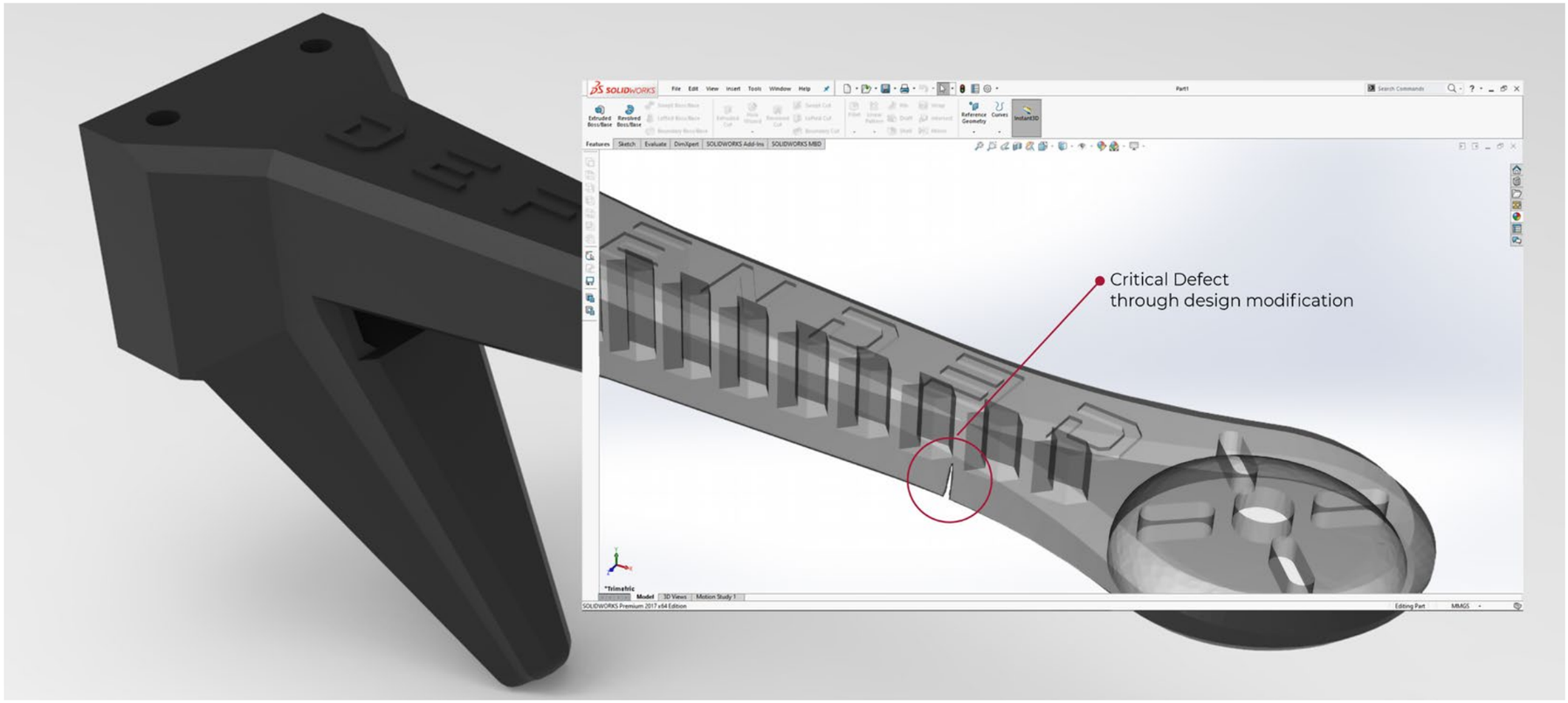


Figure 4. (Above) Examples of critical defects inserted maliciously into a design

Figure 5. (Below) Internal testing with a critical defect in the arm once printed and assembled

scope and limits of intellectual property infringements will come in time as more and more cases pass through the law courts.

3.1.6 AM Sabotage

Often many attacks can just be malicious but they would generally occur in a military context or in an adversarial situation. Attacks can occur at any vulnerable node or at multiple nodes in the AM digital process chain.

These attacks are designed to be destructive and impede an adversary's progress in sustainment in a theatre of war, thus giving the perpetrator an advantage in the military engagement.

Outside of a military scenario cyber sabotage attacks have been known to occur frequently in many sectors of the economy including the manufacturing sector. It can also result in malfunctions of equipment and secondary production processes in the full AM digital chain.

3.1.7 Manipulations

Manipulations might be considered a sub-category of AM Sabotage. In a military context this scenario is highly possible and has been shown to be an effective strategy to disable a threat from an adversary in a theatre of war.

In the future, this strategy may be used against commercial competitors of high value products to impede and reduce the quality and performance levels of their competitors' products and services. It has been demonstrated in a well known case study, the "dr0wned study". [22]

The mechanism by which this can occur is through multiple attacks at different vulnerable nodes in the full

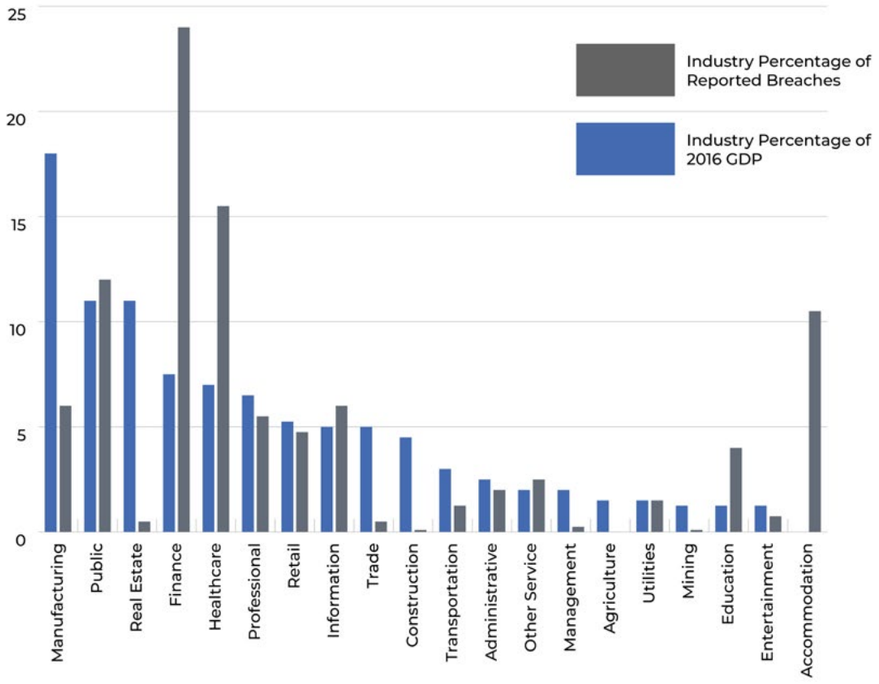


Figure 6. Education, healthcare, and finance have a higher percentage of breaches compared to their percent of the GDP. Image credit Council of Economic Advisers 2018

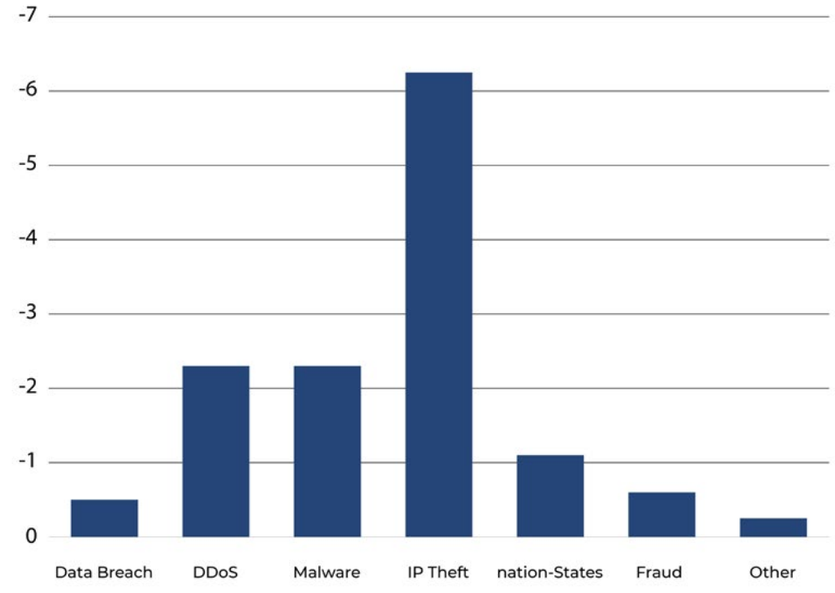


Figure 7. Percentage of negative cumulative abnormal returns for a given category of cybersecurity breach. Cybercrime is on the rise, and IP is a very costly target.[1] Image credit Council of Economic Advisers 2018

Digital Thread or pathway to manufacture. The design manipulations may not be obvious and may be inbuilt, which can significantly affect the static or dynamic fatigue fracture properties, generally aimed at the components failing prematurely and unable to take the designed loads. The consequences could be catastrophic.

DEFEND3D could Apply Azure's Kubernetes node clusters in closed environments as a governance mechanism in Virtual Networks, where there is processing of nodes and Multifactor Authentication of nodes along the AM digital chain. This could drastically mitigate attacks at any vulnerable node or multiple nodes in the process chain. Additionally, Microsoft's AI Authenticator and Deepfake Detector Tool can be repurposed for early attack detection on specific nodes and/or the whole node network.

Simulations have been undertaken by a number of academic institutions studying this form of attack. In one such simulation the institution modified the original STL file by adding hidden specific defects into the interior surfaces of the component calculated to cause the component to fail at a fraction of the design load, see Figures 3, 4 and 5.

It is likely that the modified component would pass a QA test and be used in equipment, resulting in premature failure of the equipment and facilitating the adversary's objectives. [23,24]

3.2 Cybercrime & IP Theft Costs to Industry

Wohler's Report 2021, sales of AM products and services reached $12.8 billion in 2020 and grew 7.5% despite the global Covid-19 pandemic.[25] Cybercrime is constantly increasing and so does the consequential cost to the economy. The Council of Economic Advisers (2018) stated, "malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016".

Figures 6 and 7 chart the calculations of the percent of industry reported breaches compared to the percentage of 2016 gross domestic product (GDP).

The Council of Economic Advisers (2018) shows that the costliest type of malicious cyber activity is IP theft. Metrics were gathered against a sample set of 290 security breach events, with the average loss being $498 million per cyberattack. Impact cost was based on the company stock price during a seven-day window after the cyber event was disclosed.

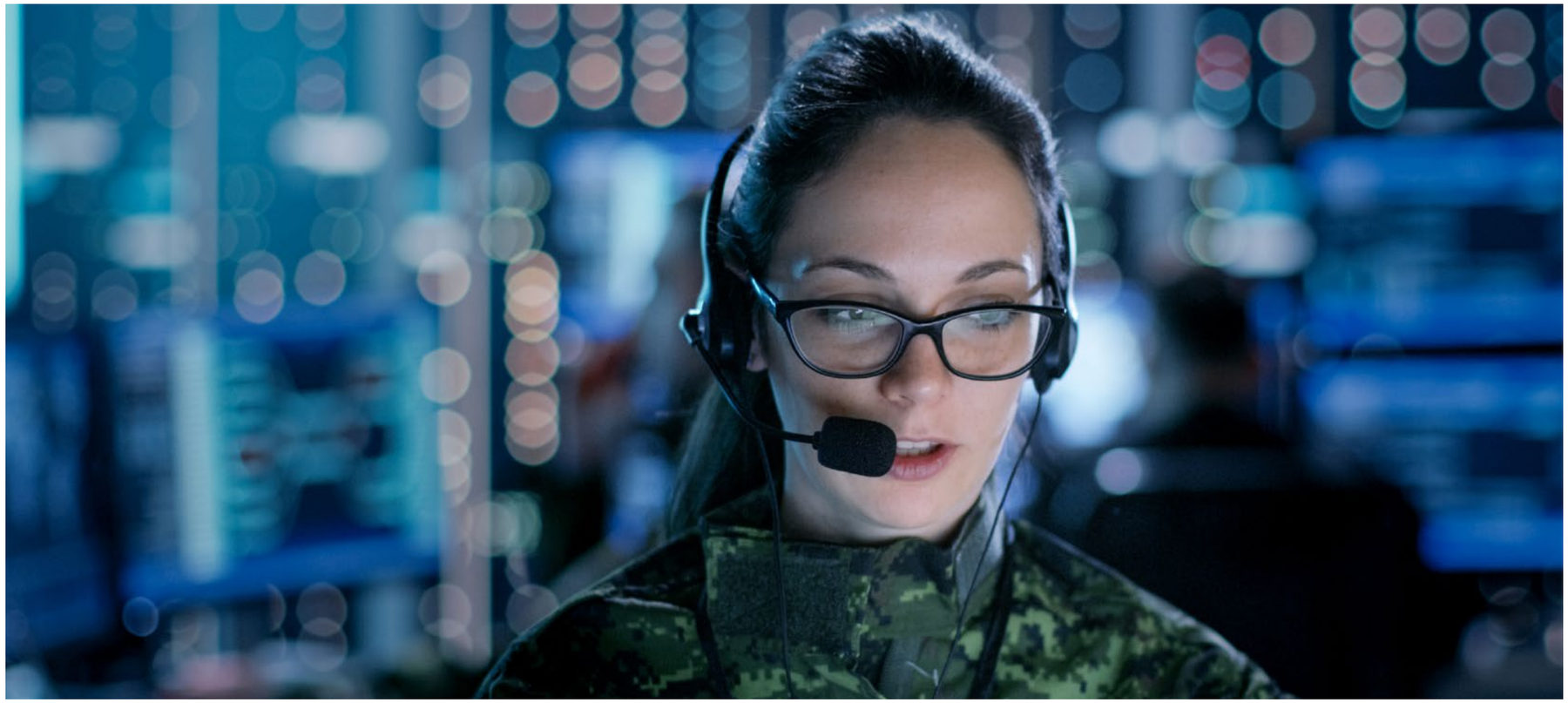
A single theft of IP data costs a company up to $498 million in reparations and lost stock value. Other than cost, negative impacts on reputation, brand equity (accelerated by the socially connected world) affects a company through loss of contracts as well.

Microsoft enables cyber trend forecasting and monitoring of malicious cyber activity with various services like specific ML models or whole infrastructure monitoring and Security Tools.

3.3 General Overview of Cybercrime in AM

The vulnerability across the entire **Digital Thread** in AM, including its physical and virtual supply chain, represents a considerable attack surface to adversaries intending to steal IP and/or do malicious harm to systems.

The same is true for Industry 4.0 - the industry vision for a digitally connected future for manufacturing. Safeguards need to be put in place in order to secure that future.



3.3.1 So what exactly is the Digital Thread?

Digital Thread
“a single, seamless strand of data that stretches all the way from the initial design concept to the finished part, constituting the information which enables the design, modelling, production, validation, use, and monitoring of a manufactured part”. [26]

For the holistic approach of securing dedicated manufacturing facilities and production processes, Microsoft Industry Cloud in combination with Digital Twins, Key Vault Storage and Virtual Networks are viable options.

The Digital Thread will include the initial digital design (CAD) to stress modelling management software like FEA, software for fatigue and fracture assessment, design orientation and slicing, through to production processes on the local LAN (local area network) such as process planning, process control, process monitoring, quality control, testing and verification processes which are often digital by nature. [27]

Tools for process analysis such as Azure Stream Analytics and Data Lake Analytics can be used to secure sensitive data along the internal chain by using VPN gateways, Azure Data Share and VMs for creating, processing and storing sensitive data like CAD files.

To support the workforce in secured facility operations, Cognitive Services can be applied for efficient monitoring, testing and verification processes.

The Digital Thread can be more complicated when the 3D printing is outsourced. In this case the manufacturer’s digital thread including their LAN and their supply chain can be incorporated, thus introducing an additional attack surface and vulnerability within the entire digital thread for the component to be manufactured.

The Digital Thread is even more vulnerable if the digital 3D printing files have to be sent to a remote site in a theatre of war to be manufactured using subtractive and/or additive processes.

DEFEND3D presents a solution to this exact problem in this paper. Files never have to be sent to the remote location and no trace of any 3D print file or residual data will remain in the AM process system.

3.3.2 What are the AM Vulnerabilities within the Complete Digital Thread?

Do et al. [28] tested and analyzed the security of two MakerBot 3D Printers, the Replicator (5th gen) and Replicator Mini. Both these machines can be connected via Ethernet, Wi-Fi, or USB.

The results of their study of the communication protocol indicate that an adversary on the local network will be able to retrieve current and previously printed 3D print file models.

The attackers can exploit vulnerabilities in the protocol by obtaining credentials (authentication code and client secrets) which could be used to send commands to the 3D Printer. It is possible to stop an active printing job or submit a new one. The network protocol also makes it possible to retrieve the last submitted print job.

To avoid AM vulnerabilities within the digital thread, Azure Stack services can be combined (depending on the network) with Virtual Networks, VM Instances and Containerization for backup services.

The authors perform a static analysis of the source code and a dynamic analysis of communications

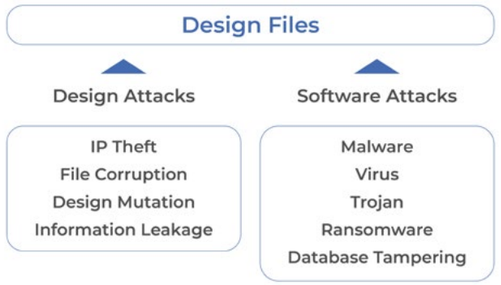


Figure 8. Attacks in the design stage in the supply chain of AM components [40]

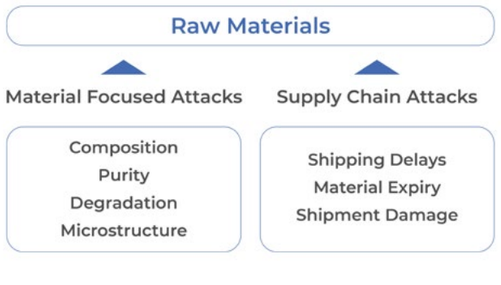


Figure 9. Attacks on raw materials in the supply chain of AM components [40]

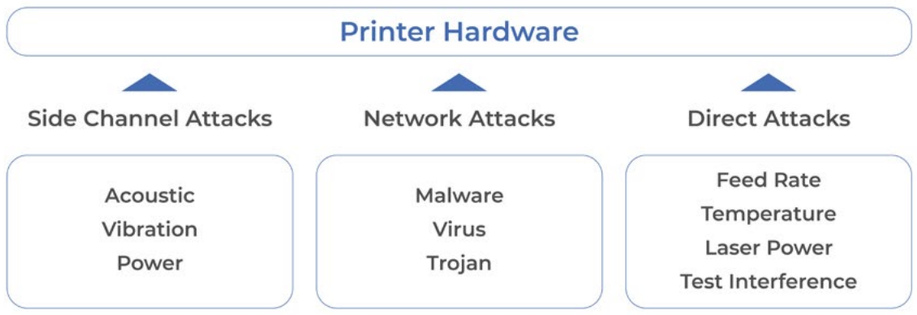


Figure 10. Attacks on printer hardware in the supply chain of AM components [40]

between the 3D Printer and computer. Numerous exploitable vulnerabilities were present, including the use of fixed size local buffers in combination with potentially unsafe functions like sscanf and memcpy.

Pope et al. [29] apply the Systems-Theoretic Process Analysis (STPA) framework [30] to hazard analysis in AM. The authors show that this approach can be used to systematically identify manipulations that can be used to sabotage the manufactured part.

The real-time analysis of vulnerabilities in the network and/or between 3D Printer and computer is supported by HDinsight, High-Performance Computing Cache, Data Lake Analytics and Azure Stream Analytics can be deployed securely for quick results.

Timing disruptions in the control loop have potentially hazardous defects; sensor readings and commands that are provided too late, too soon, or out of order are also vulnerabilities. By disrupting the power supply to the 3D printing process the printed object can be sabotaged.

3.3.3 What is an Attack Vector?

Attack vectors, as defined by Souppaya & Scarfone (2016) [31], are “segment[s] of the entire digital thread that an attack uses to access a vulnerability.” An attack vector primarily contains a source of malicious content, a vulnerable processor and the malicious content itself.

Essentially, it is the method a hacker uses to gain access to networks or computers. A malware payload is then delivered once the vector is successful. One analogy for attack vectors is a guided missile where the payload is the warhead at the tip (Rouse, Attack Vector, 2012). [32]

List of attack vectors:

- Cyber supply chain [33]
- Phishing e-mail (attack vector) with a malicious attachment [dr0wned study] [22]
- Automated malware (e.g., Computer Worm) [4,22,34]
- Bugs in 3D Printer software, firmware, Network Protocol [34]
- Code Injection [35]
- Open access of machines to internet, for firmware updates and maintenance [36]

Souppaya & Scarfone (2016) [31] went on to detail further examples of attack vectors:

- Malicious web page content (content) downloaded from a web site (source) by a vulnerable web browser [1]
- A malicious email attachment (content)in an email client (source) rendered by a vulnerable helper application (processor) [1]
- A malicious email attachment (content) downloaded from an email server (source) to a vulnerable email client (processor) [1]
- A network service with inherent vulnerabilities (processor) used maliciously (content) by an external endpoint (source) [1]
- Social engineering-based conversation (content) performed by phone from a human attacker (source) to get a username and password from a vulnerable user (processor) [1]
- Stolen user credentials (content) typed in by an attacker (source) to a web interface for an enterprise authentication system (processor). [1]
- Personal information about a user harvested from social media (content) entered into a password reset website by an attacker (source) to reset a password by taking advantage of weak password reset processes (processor). [1]

The dr0wned study [22] is an example of a malicious attack that shows the stages of an attack from finding a vulnerability in a computer system to the execution of the attack and achieving the adversary’s objective of sabotage. In this study all the elements of the sabotage attack are illustrated from exploiting an attack vector through to the attack itself on the target. A phishing e-mail (attack vector) with a malicious attachment was sent to a 3D Printer owner. The attachment was designed to exploit a known cyber vulnerability and to install a reverse shell backdoor on the computer (compromised element). The same computer was used to submit jobs to the 3D Printer (thus acting as the Controller PC).

Turner et al. [37] conducted a study of additive and subtractive manufacturing processes and identify attack surfaces. The results of their study showed that manufacturing systems contain several attack vectors that can be easily exploited.

The authors note that manufacturing machines have no physical or common cybersecurity. Design files are generally transferred via non-secure communication mechanisms like e-mails or USB drives. These design files commonly do not incorporate any security mechanisms to verify their integrity.

A method to detect various kinds of attack vectors in manufacturing machine systems and supply chains is to setup the Adversarial ML Threat Matrix. This is done with the support of Microsoft Defender Advanced Threat Protection (ATP) integrated in Azure Security Center in combination of AI/ML specific threats and their Mitigations Modelling.

Integrated Azure Stream Analytics and Data Lake Analytics reinforce these security measures.

3.3.4 Attack Methods

Cybersecurity attack methods include:

- 3D Part’s External Shape/Size (impacts part’s fit) [35]
- Insertion of Internal Defects (voids or critical defects) [4,34,36,38]
- New Print Job Submission [39]
- Print Job Cancellation [28]
- Print Job Substitution [34]

Figures 8, 9 and 10 characterize the types of attacks that can occur at these locations. At the design level, software attacks can result in IP theft, file corruption, design mutations and information leakage [39] using Malware, viruses, Trojan Ransomware and database tampering. [4,34,36] At the 3D Printer hardware level, direct attacks can result in the alteration

Due to the cyber-physical nature of AM, **supply chain risk management** of the AM process **needs to be undertaken**.

of the process parameters, feed rate, temperature changes, laser power intensity modification, sabotage, denial of service or print job cancellation. [34,40] This can be achieved using malware, viruses and Trojan software.

Side channel attacks can also impact the printer by attacks and manipulation of the peripheral resources that the printer needs like power. By attacking a smart meter in the power line the hacker can shut down the printer directly and cause physical defects in the printed object. [40]

Adversaries could take control of thousands of 3D Printers that can be accessed directly from the Internet without requiring any authentication. According to the SANS Internet Storm Center, a Shodan search reveals over 3,700 instances of OctoPrint interfaces exposed to the Web, including nearly 1,600 in the United States. [41]

OctoPrint is an open source web interface for AM machines. It gives owners remote access to their printers to monitor and control the progress of their build which is used to start, stop or pause a printing activity. It can also allow access to the printer's webcam.

Attackers can access and alter the G-code files, which are files that contain the design and the instructions used to print a 3D design. For large companies these files may contain details of new product innovations that need to be kept secret. [41]

Raw material attacks focus on the logistics of the supply chain where an attack may cause delays in shipment of raw materials. Hacks in the supply chain can cause substitution from high quality powders ordered to low quality powders or counterfeit powders in the orders. [40]

3.3.5 Compromised Elements of the Digital Thread

Compromised elements can include:

- Overall Cybersecurity
- 3D Printer Firmware [34,35]
- Computer Network (Wi-Fi) [28]
- Controller PC [4,23,34,38,42]
- Physical and Virtual Supply Chain [40]

Each Digital Thread should be secured with appropriate tools like Azure Digital Twins, Azure Stack for supply chain motions (i.e. process machines, Edge Computing), VM Environments and Gateways as well as Private Networks for end-to-end communication.

This is to mitigate compromised elements of the Digital Thread.

3.3.6 Remote Printing Risks in Cybersecurity

Some equipment manufacturers and owners require remote access to 3D Printers for setting up, calibration and to perform firmware updates. It can also be a requirement to support troubleshooting and maintenance.

This can potentially become a significant vulnerable site with a large attack surface profile if there are no appropriate security measures in place.

Glavach et al, [36] report an incident where a $750,000 dual-laser 3D Printer was connected to the internet via an open connection, normally provided to corporate guests.

The OEM could have remote access to the printer, without the owner noticing. The remote access protocol uses default settings, and was unencrypted. [36]

"**Cybersecurity is another concern moving forward**. We don't want adversaries to get into our files and download our spare parts. Or to make counterfeit parts that [...] are engineered to fail [...] And we do not want internal flaws in the printing that could degrade our weapon systems."

Lt. General Aundre Piggee - US Army/G4 - 2019

The consequences of this vulnerability may result in a direct attack on the 3D Printer itself. [4,8,23,43]

The attacker might install malware, Trojans and viruses into the printer software potentially gaining access to confidential design and process parameters. [34,35]

Alternatively, if the hack is malicious all kinds of damage might be inflicted as the attacker would be able to change the critical process parameters at will in a deleterious way which might manifest itself in the production of critical defects in the printed parts. The hack could also disrupt the production by shutting down the systems and denying access to the printer.

A straightforward theft of the design file might ensue, resulting in thousands of illegal products being printed and sold in the same market as the genuine OEM, dramatically reducing their sales.

To secure the remote equipment access Multifactor Authenticator, VM Instances for remote update processes and Key Vaults can be set up easily.

3.3.7 What are the Possible Consequences of an Attack?

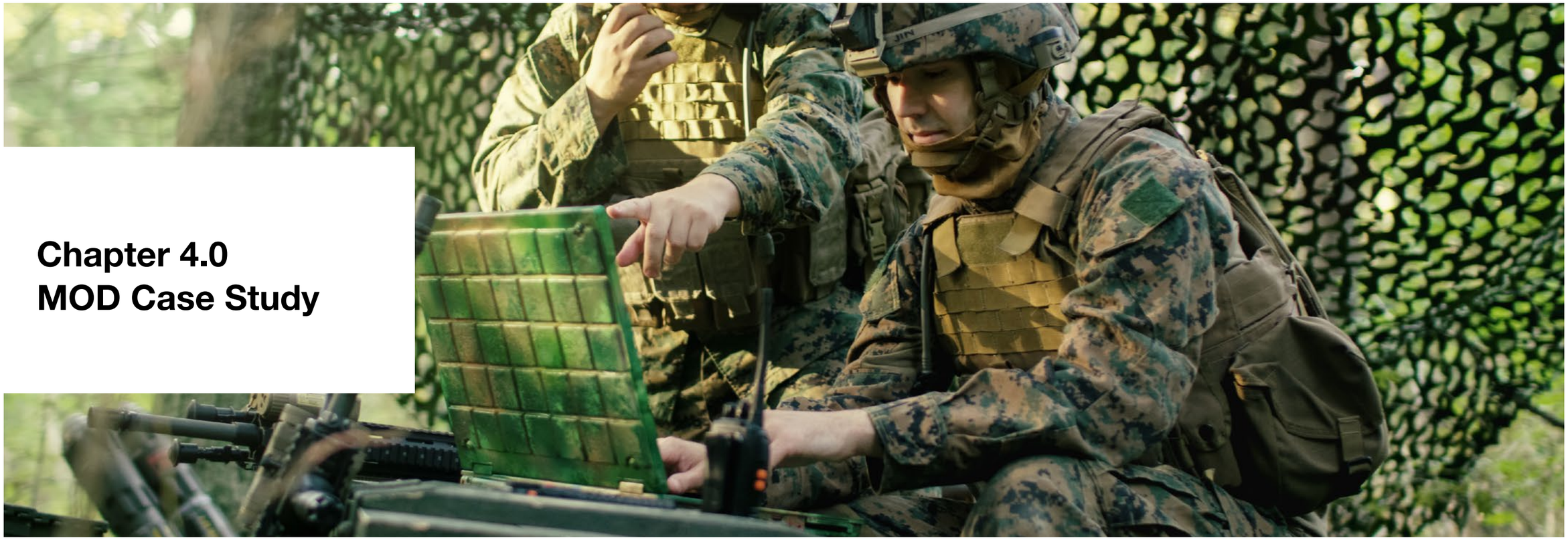
The consequences of attacks on vulnerabilities in the Digital Thread of the AM industry (including its physical and virtual supply chain) can result in technical data theft, industrial espionage, IP theft, counterfeiting, reverse engineering, AM sabotage and manipulations.

Cyberattacks can translate to reduced manufacturing productivity, reduced manufacturing efficiency, reduced product performance, lower profits, loss of IP, substandard parts, various safety issues, a lowering of the company image (potentially leading to loss of consumer confidence) and reduced brand equity for the company.

Due to the cyber-physical nature of AM, the Supply Chain Risk Management (SCRM) of the AM process needs to be undertaken. [40] SCRM frameworks involve stages of risk identification, risk assessment and risk mitigation. [44]

Supply chain risks could be identified, assessed and mitigated quicker and more effectively with the implementation of:

- Microsoft Cloud for Manufacturing
- Digital Twins
- Digital Threads as the digital backbone for the utilization of Azure Data Lake Analytics
- Azure Stream Analytics and API Management to supply chain player's systems as well as third party data provider (for example, weather forecast databases).



Chapter 4.0
MOD Case Study

4.1 DEFEND3D - A New Patented Technology

DEFEND3D is a new and patented technology for the transmission of remote 3D printing, CNC machining, laser cutting, Bioprinting and other digital manufacturing data with One-Click-Print. The solution encompasses the method for controlling reproduction of an item represented by a digital asset stored in a trusted computing environment using a reproduction device in an untrusted computing environment.

This game changing cybersecurity and transmission protocol enables a secure digital resupply of reproduction parts to remote locations without the necessity of any file transfer. This is done by a continuous stream of production instructions to the machine. These reproduction instructions are secured by six levels of security, encryption being only one of them. All manufacturing jobs are recorded in detail, providing an audit trail throughout the entire digital supply chain. Variables such as machine settings, type of machine, type of material, etc. can be set to enforce manufacturing standards and to ensure the highest quality in the production process.

DEFEND3D has been tested by UK Strategic Command, a division of the UK Ministry of Defence (MOD), where provision of a Secure Platform for Digital Manufacturing has been delivered.

The platform links up a central design hub in a secure facility with multiple deployed locations that do not have engineering specialists. There is no trace of the 3D file left on the 3D Printer or computer.

Microsoft Azure Cloud computing enables secure information sharing across services, domains, and the allied community - all the way from headquarters

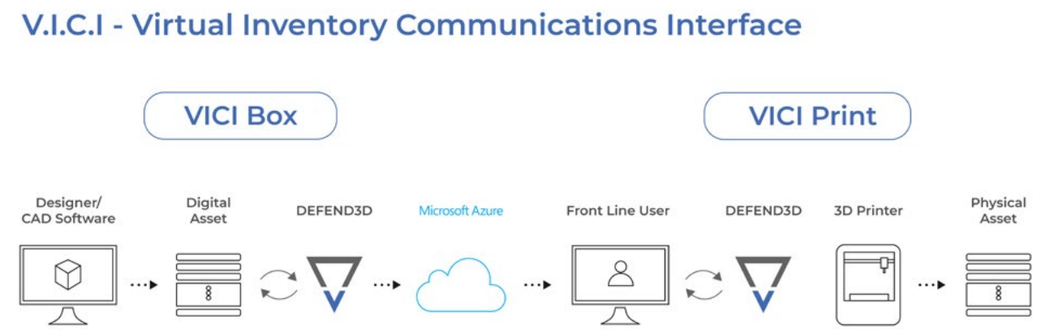
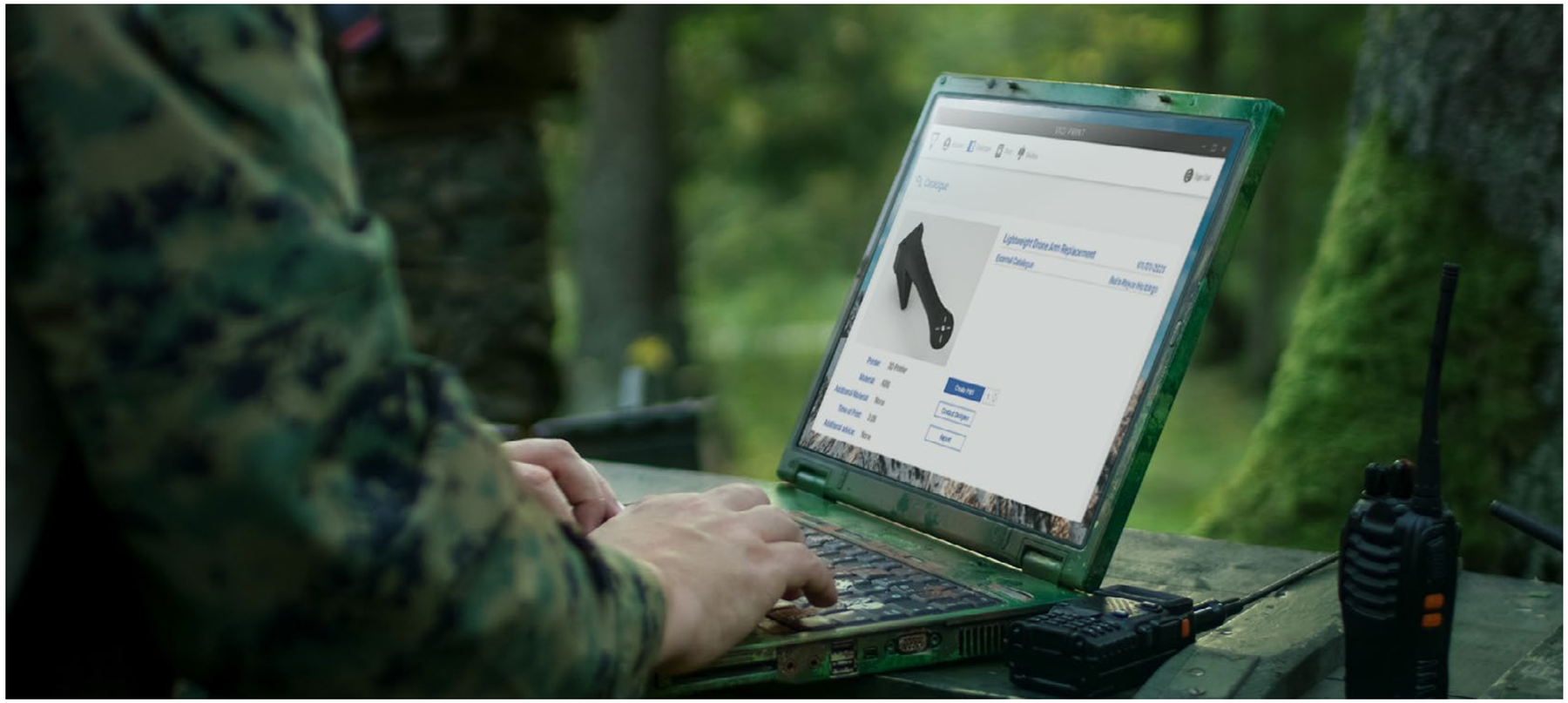


Figure 11. DEFEND3D Software. End-to-end encryption securely delivering virtual inventory



to the tactical edge and to the soldier at a forward-deployed location. [45]

Services such as Azure Remote Rendering provide an AI based solution for 3D Printer remote management and monitoring which can support DEFEND3D's solution appliances. Applying IoT services for DEFEND3D's customer can enhance the solution's operations in synchronicity with customer's operations.

4.2 Testing & Performance Requirements

a. 3D Print Engineering Support

i. Quality – The quality of the product delivered at the deployable end of the DEFEND3D network will be just as good as the 3D print on the same printer at the base location. To test this, two exact prints will be compared. One through DEFEND3D and one printed locally. Once both prints have been completed, the quality of the print will be compared visually and scientifically.

The visual inspection will be carried out by a fully qualified precision engineer within UK Strategic Command. The science test will be carried out by both prints being subjected to tensile and compressive strength evaluation through a tensometer operated by UK Strategic Command precision engineers.

DEFEND3D could utilize Azure Stack and Azure Security Services for secure communication between the Strategic Command Center and the 3D Printers' Visual inspections for testing purposes. This could be supported by the Microsoft Deepfake Detector Tool for counterfeit products. Scientific testing can be accelerated with Azure Cloud Computing/High Performance Computing.

ii. Time – The time taken to print out an STL file through the DEFEND3D network must be comparable with the time taken to print out the same file locally.

To test this, the DEFEND3D solution will use a virtualized network with a low data link of 256kbps with a low error rate and relative latency (3000 mile distance).

The DEFEND3D distant location will begin printing through this network at the same time that the same file is printed separately from a locally connected UK Strategic Command design station and Engineering Grade 3D Printer. Once each print is completed, a time comparison will be documented.

The DEFEND3D solution to compare printing time could utilize Azure Cloud Computing for monitoring and securing the data transfer via Azure Virtual Networks and VPN Gateways.

iii. Assistance – All warnings, guidance and indicators normally available to a locally connected Engineering Grade 3D Printer not using the DEFEND3D network must be accessible and available to the end user of the DEFEND3D solution.

b. Communications Security and Adaptability and Data Security at Rest

i. Data Security – No data files pertaining to prints delivered at the distant end of the DEFEND3D network will be in existence on the user device or within the 3D Printer chipset. The design of the DEFEND3D network is such that it is not the data file that is physically transmitted in which case this means that no data at rest should be seen at the distant end. Once a file has been physically transmitted during the demonstrations, a UK Strategic Command communications engineer will search the user device and printer for any residual data that would indicate what sort of file was transmitted.

"We assess this [**DEFEND3D** technology] to be a **game changing capability**, allowing us to overcome our current reticence of sending sensitive parts overseas, and allow us to send more parts wherever we wish in the world. Being familiar with cutting edge 3D printing technologies, I believe this to be the **only such system on offer**."

Lt. Col. ********** - MOD

ii. Adaptable Communications – Due to the manner in which the file is transferred across the DEFEND3D network to the 3D Printer, it is suggested that low data rates could be used without any effect on the data integrity or speed of the actual print at the distant end. UK Strategic Command communications engineers will manipulate the data network used for the experimentation. Link budget will be tested at 100MBps, 50MBps, 2 Mbps, 256Kbps, 56Kbps, 19.2Kbps, 9.6Kbps. DEFEND3D could utilize temporary VPN Gateways to ensure adaptable communications on various data rates.

c. Usability

i. Data Format Capability – The DEFEND3D application will not restrict the size of the file, only restriction will be as to the size of the hardware storage space. If a large file is being selected for print however, as stated above, an indicator of the time expected to print should be available to the distant user. The DEFEND3D application will be downloadable on all standard Windows machines and laptops.

ii. Training Burden – The application should require no more than one hour's training to be proficient at the deployed location. All commands and access should be easy to follow and intuitive. This will be accessed subjectively by UK Strategic Command user community.

d. Test Equipment

An Ultimaker 2+ 3D Printer was used for all key performance indicator (KPI) 3D printed test samples. A standard tensile test piece was used for continuity, simplicity and time to print. A universal tensile testing machine (10 kN load capacity) was purchased and was used for all tensile strength investigations.

4.3 Summary of Results

This summary describes the testing undertaken by the mechatronics team to compare the quality of a component produced from the DEFEND3D network (in the scenario of being at the deployed location) to the quality of the print at the base location. This arrangement was devised to simulate how the deployed user can be supported from the base location, with the base location providing the functionality of a virtual engineer. Below describes the testing procedure, the equipment used, and the results obtained from the 3D printed components under the two slightly differing processes.

Benchmark testing with the MOD shows that printing time and quality is not affected when using the DEFEND3D transmission service, even when compared to the print from an SD card. Throttling of the bandwidth down to 56 kb/s proved successful with fully completed prints being reproducible at this speed. Three standard tensile test pieces were printed off at three different thicknesses, 3mm, 5mm, 8mm. Visually, there was no significant difference between components printed through the DEFEND3D network and those printed via the SD card. To confirm the physical appearance more scientifically, thickness measurements were taken of the the tensile sample test pieces using Vernier calipers.

A repeat test using pre-sliced G-code parts through DEFEND3D also showed positive results with minimum variation between thickness. Testing results established no access to the original 3D file and no residual data to be found within the 3D Printer chipset. All tests were triplicated.

To conclude, the solution proved equal to SD card prints, low bandwidth, and most importantly, no data at rest.

Chapter 5.0
Discussion

This paper introduced the latest status with regard to AM applications in the Air Force, Navy and Army. It is clear that more AM printed components are being incorporated into flight critical and high end military operations. This raises the engineering confidence levels for AM applications in these sectors for further expansion into more critical applications in the future.

The second chapter reviewed the issue of cybercrime and IP theft in AM. Examples were given of how cybercrime has negatively impacted commercial operations of companies and institutions. The cybercrime review also identifies the areas where AM operations are most vulnerable and where actions are needed to secure and protect the integrity of AM and its supply chain.

It is estimated that 90% of a company's environmental impact is due to its supply chain, with £56 billion per annum in extra costs to British businesses due to supply chain disruption. A case in point is the March 2021 blockage of the Suez Canal by the ship Ever Given, operated by Evergreen.

Blockchain encryption has recently been proposed as a solution to some of the vulnerabilities within the Digital Thread. Blockchain has its merits but it also introduces a number of restrictions and disadvantages.

An industrial conglomerate submitted a patent application in 2017 outlining a method for integrating blockchains into AM to create a database that validates and verifies the manufacturing process to verify 3D printed parts in its supply chain. Ideally, this could tackle existing challenges in the current systems for AM which "lack verification and validation systems for ensuring that objects produced by the process are appropriately certified," according to the application. The concern here is if a replacement part for an industrial asset is produced using an AM process, anyone with access to a 3D Printer could reproduce that part. As a result, end users cannot verify whether the replacement part "was produced using a correct build file, using correct manufacturing media, and on a properly configured AM device." [46]

3D printing has a growing need for cybersecurity with significant safety hazards due to counterfeit parts or products being deliberately printed with hidden failures in the Digital Thread. Blockchain offers security for transport when it comes to 3D data, by breaking the file in to blocks, and applying hashing algorithms to the block and its previous block to account for any file manipulation.

To mitigate this, blockchains have something called proof-of-work, which slows down the creation of new blocks where it calculates the required proof-of-work and adds new blocks to the chain. This makes blockchain a very inefficient way for the data transport of 3D files, especially for larger files due to the time it takes. By contrast DEFEND3D is streaming directly to a 3D Printer in real time and only provides information to the printer that is necessary in the moment.

By utilizing blockchain within industry for AM, OEMs would still need to share their IP or Digital Asset and digital inventory across the platform by sending the file. Also, the entire 3D file will still arrive at the printer making it possible to intercept.

The DEFEND3D solution prevents file transfer while still offering authentication such as hashing algorithms to ensure the integrity of all data whilst offering a better security solution for the 3D file.

With DEFEND3D the IP or full digital asset is completely retained by the owner and is never sent. DEFEND3D has multiple mechanisms in place to detect any sniffing activity or an imminent attack, if detected, this will alert and shut down the printing job.

There are many solutions claiming to help solve the IP and cybersecurity concerns in AM. An iTunes approach has recently been proposed allowing companies to “license the use of the CAD data required to print replacement parts.”

Equally, the US DoD is currently exploring a similar approach as published in their strategy to make AM a more generally accepted technology.

“To mainstream AM across the DoD, five primary needs must be addressed:

1. Rapid and standardized approaches for qualification of materials and processes, and certification of AM parts
2. New business models for the contracting and acquisition of AM digital technical data
3. Logistics model for production of AM parts at forward operating locations
4. Standard AM technical data content
5. An interoperable and secure AM digital thread for connectivity and data management.”

“DoD will consider technical data access as part of the contracting process, to include alternative business models such as licensing rather than acquiring data”.

However, licensing of digital data from OEM suppliers is far from desirable. This solution might help the DoD obtain access to parts for point of need printing on demand and replace obsolete parts but it does not negate the vulnerability risk of the entire transfer of the digital file.

Moreover, it still remains to be seen whether OEM suppliers who have spent considerable resources into R&D will actually allow some of their most sensitive digital data to be transferred in practice. [47]

One US company aims to deliver an integrated solution to provide advanced security, quality assurance and traceability for the digital supply chain by merging manufacturing instructions with a set of licensing and production meta-data specified by the designer. This assists to track a product from its earliest design, into production ensuring products are manufactured and authenticated to exact specifications.

Their product suite encrypts, distributes, and traces the digital flow of parts to prevent counterfeit parts and ensure that manipulated parts cannot enter the physical supply chain. The main goal is traceability but to ensure delivery of data, the whole file is still being sent, allowing for loss of digital IP and redistribution if accessed.

The DEFEND3D solution does not send 3D files but allows a digital asset to be live streamed to a 3D Printer in real time, providing only necessary information to be accessed at any time before instantly deleting processed information.

Chapter 6.0
Conclusion

The importance of AM within the Defense sector is growing significantly amongst governments who are adopting the technology into their operations, maintenance and logistics. There is a clear consensus that the threat of cybersecurity vulnerabilities to IP is very real and present.

A new patented solution called DEFEND3D has been introduced, that protects the owners' IP in such a way that it is now no longer necessary to send digital assets (i.e. the digital print files) to external manufacturers. Retention of the IP is now assured and retained.

This is particularly true for military digital assets that are far too sensitive to be shared externally. DEFEND3D has been tested by the UK Strategic Command division of the MOD, where provision of a Secure Platform for Digital Manufacturing has been delivered. All other attempts to solve the IP and cybersecurity risks still involve the transfer of the entire digital file.

Only DEFEND3D's solution protects OEM's digital inventory because the file never leaves due to the way it is streamed to the 3D Printer. This creates an opportunity for Defense and Industry to collaborate without compromising on the transfer of sensitive data.

DEFEND3D's end user software application, VICI Print, has been designed with a low training burden, meaning the user does not have to be an engineer or AM expert. By browsing the catalogue they are simply able to One Click Print. This will lead to further democratization of AM as a capability in remote locations.

DEFEND3D has been found to be a successful and effective end to end encryption software tool for controlling reproduction of a digital asset stored in a trusted computing environment using a reproduction device in an untrusted computing environment.

"Training to an unskilled user was successful. Within 30 minutes, they were able to select a file from the catalogue, upload it to the print queue and then follow the instructions to commence a print. **This proves the VICI Print software is intuitive and simple to operate minimizing the training burden**."

Head of Mechatronics (MOD)

Strategic Command

"You won't find it difficult to prove that battles, campaigns, and even wars have been **won or lost** primarily **because of Logistics**"

General Dwight D. Eisenhower

Get in Touch

DEFEND3D is the leading manufacturing solution enabling secure transmission for remote 3D printing with One-Click-Print. Our patented security protocol delivers end-to-end encryption allowing organizations to store their designs locally on their home server while enabling them to use their virtual inventory to manufacture parts in remote locations without any file transfer and with no data at rest. Our clients often operate within special and challenging conditions, requiring bespoke secured solutions to be delivered as fast as they are needed. To discuss integrating DEFEND3D into your digital supply chain, please contact Anisha Singh, our CPO, to find out more.

Anisha has been at the forefront of the DEFEND3D solution and plays a vital role in product management, innovation, and development. With a degree in Computer Science and Robotics, she has spearheaded working on bespoke mechatronic systems for industrial, medical and laboratory use, providing services for design, rapid prototyping, and manufacturing, and now bringing disruption to digital manufacturing with the DEFEND3D solution.

Anisha Singh, CPO, DEFEND3D

info@defend3d.com

Bibliography

1. Cpl. Bjorndal, D (2012). VERTICAL REPLENISHMENT, U.S. Marine Corps photo. Retrieved from https://www.marines.mil/Photos/igphoto/2001632365/?igsearch=MH-60S%20Sea%20Hawk%20Alexis%20Flores

1. Scott, M. L. (2019). Preventing intellectual property theft in Additive Manufacturing

2. Kurfess, T., & Cass, W. J. (2014). Rethinking Additive Manufacturing and Intellectual Property Protection. Retrieved from https://www.researchgate.net/publication/265173110_Rethinking_ Additive_Manufacturing_and_Intellectual_Property_Protection

3. Widler, M., & Rajan, V. (2016). 3D opportunity for intellectual property: Additive Manufacturing stakes its claim. Retrieved from https://www2.deloitte.com/content/dam/insights/us/articles/3d-printing-intellectual-property- risks/ER_2981-3D-opportunity-intellectual-property_MASTER.pdf

4. Yampolskiy, M., King, W. E., Gatlin, J., Belikovetsky, S., Brown, A., Skjellum, A., & Elovici, Y. (2018). Security of Additive Manufacturing: Attack taxonomy and survey. Additive Manufacturing, 21, 431-457

5. Yampolskiy, M., Andel, T. R., McDonald, J. T., Glisson, W. B., & Yasinsac, A. (2014). Intellectual property protection in Additive Layer Manufacturing: Requirements for secure outsourcing. Retrieved from https://www.researchgate.net/publication/301466450_Intellectual_Property_ Protection_in_Additive_Layer_Manufacturing_Requirements_for_Secure_Outsourcing

6. Campobasso, T. (2015). Super soldiers: 3D bioprinting and the future fighter. Journal Article| Dec, 8(6), 23am.

7. Essop, A. (2020). NSCRYPT'S RUGGED FACTORY IN A TOOL 3D PRINTER DEMONSTRATED TO U.S. ARMY. Retrieved from https://3dprintingindustry.com/news/nscrypts-rugged-factory-in-a-tool-3d-printer-demonstrated-to-u-s-army-168962/

8. Jackson, B. (2019). U.S. Army secretary places 3D printing center of modern policy. Retrieved from https://3dprintingindustry.com/news/u-s-army-secretary-places-3d-printing-center-of-modern-policy- 162893/

9. Arcano, T., Bouffard, B., Marotto, H., Wood, C., Freidell, M., Frazier, W., . . . Hayleck, R. (2017). Department of the Navy (DON) Additive Manufacturing (AM) Implementation Plan V2. 0 (2017). Retrieved from Defence Technical Information Center. https://apps.dtic.mil/sti/pdfs/AD1041527.pdf

10. Vialva, T. (2019). UK Ministry of Defence to leverage 3D printing in new security approach. Retrieved from https://3dprintingindustry.com/news/uk-ministry-of-defence-to-leverage-3d- printing-in-new-security-approach-161491/

11. Meyers, M. (2016). Osprey takes to the sky with 3-D printed critical parts. Retrieved from https:// www.navytimes.com/news/your-navy/2016/08/01/osprey-takes-to-the-sky-with-3-d-printed-critical- parts/

12. Keane, P. (2020). Digital Twins and 3D Printing for Army Helicopters. Retrieved from https://3dprinting.com/aerospace/digital-twins-and-3d-printing-for-army-helicopters/

13. Svan, J. (2019). Metallic 3D Printing May Revolutionize Maintenance for F-22 Raptor. Retrieved from https://www.military.com/daily-news/2019/01/19/metallic-3d-printing-may-revolutionize- maintenance-f-22-raptor.html/amp

14. O'Neil, B. (2015). Israeli Military Now 3D Printing Drones With American-made Printers. Retrieved from https://3dprint.com/86114/israelis-3d-printers-robots/

15. Erwin, S. (2017). Marines take 3D printed drones from the lab to the field. Retrieved from https:// defensesystems.com/articles/2017/05/08/marinecorpprint.aspx?m=1

16. Army, B. (2020). British army to use 3D-printed high explosives. Retrieved from https://www. armyrecognition.com/weapons_defence_industry_military_technology_uk/british_army_to_use_3d- printed_high_explosives.html

17. Malyasov, D. (2019). U.S. Marine Corps plans to use 3D-printed impellers on Abrams tanks. Retrieved from https://defence-blog.com/news/army/u-s-marine-corps-plans-to-use-3d-printed- impellers-on-abrams-tanks.html?amp

18. Burns, S., & Zunino, J. (2017). Researchers fire 3-D printed ammo out of a 3-D printed grenade launcher. Retrieved from https://asc.army.mil/web/news-alt-amj17-rambos-premiere/

19. Louis, M. J., Seymour, T., & Joyce, J. (2014). 3d opportunity for the department of defense: Additive Manufacturing fires up. A Deloitte Series on Additive Manufacturing, 18-19.

20. Sertoglu, K. (2021). Dutch Navy boosts spare part production with INTAMSYS 3D printer tech.Retrieved from https://3dprintingindustry

21. Brothers, E. (2021). ExOne to develop portable 3D printing factory. Retrieved from https://www.aerospacemanufacturinganddesign.com/article/exone-develop-portable-3d-printing-factory/

22. Belikovetsky, S., Yampolskiy, M., Toh, J., Gatlin, J., & Elovici, Y. (2017). dr0wned–cyber-physicalattack with additive manufacturing.

23. Yu, S.-Y., Malawade, A. V., Chhetri, S. R., & Al Faruque, M. A. (2020). Sabotage attack detection for Additive Manufacturing systems. IEEE Access, 8, 27218-27231.

24. Zeltmann, S. E., Gupta, N., Tsoutsos, N. G., Maniatakos, M., Rajendran, J. and Karri, R. "Manufacturing and security challenges in 3D printing," JOM, vol. 68, no. 7, pp. 1872–1881, Jul. 2016.

25. Everett, H. (2021). Wohlers Associates publishes 2021 annual State of 3D Printing report. Retrieved from https://3dprintingindustry.com/news/wohlers-associates-publishes-2021-annual-state- of-3d-printing-report-186439/

26. Trouton, S., Vitale, M., & Killmeyer, J. (2016). 3D opportunity for blockchain: Additive manufacturing links the digital thread. In: Deloitte University Press.

27. Nassar, A. R., & Reutzel, E. W. (2013). A proposed digital thread for additive manufacturing. Solid Freeform Fabrication, 19-43.

28. Do,Q., Martini, B., Choo, K.-K. R., A data exfiltration and remote exploitation attack on consumer3d printers, IEEE Transactions on Information Forensics and Security 11 (10) (2016) 2174-2186.

29. Pope, G., Yampolskiy, M., A Hazard Analysis Technique for Additive Manufacturing,in: Better Software East Conference, 2016, p. 17. URL http://arxiv.org/abs/1706.00497

30. Leveson, N., Thomas, J,. An STPA primer, MIT Press, 2013. URL http://psas.scripts.mit.edu/home/wp- content/uploads/ 2015/06/ STPA-Primer-v1.pdf

31. Souppaya, M., & Scarfone, K. (2016). Guild to Data-Centric Threat Modeling. NIST Special Publication, 1-20. Retrieved January 19, 2019, from https://csrc.nist.gov/CSRC/media/Publications/sp/800- 154/draft/documents/sp800_154_draft.pdf

32. Rouse, M. (2012, May). Attack Vector. Retrieved from searchsecurity.techtarget.com: https:// searchsecurity.techtarget.com/ definition/attack-vector

33. Yampolskiy, M,. Skjellum, A., Kretzschmar, M., Overfelt, R. A., Sloan, K. R. Yasinsac, A. Using 3D Printers as Weapons, International Journal of Critical Infrastructure Protection 14 (2016) 58-71.

34. Moore, S., Armstrong, P., McDonald, T., Yampolskiy, M. Vulnerability analysis of desktop 3d printer software, in: Resilience Week (RWS), 2016, IEEE, 2016, pp. 46-51.

35. Xiao Zi Hang (Claud Xiao), Security attack to 3d printing, keynote at 2070 XCon2013 (2013). URL http://www.claudxiao.net/ Attack3DPrinting-Claud-en.pdf

36. Glavach, D., LaSalle-DeSantis, J., Zimmerman, S. Applying and assessing 2160 cybersecurity controls for direct digital manufacturing (ddm) systems, in: Cybersecurity for Industry 4.0, Springer, 2017, pp. 173-194.

37. Turner, H., White, J., Camelio, J. A., Williams, C., Amos, B., Parker, R. Bad parts: Are our manufacturing systems at risk of silent cyberattacks?,IEEE Security & Privacy 13 (3) (2015) 40-47.

38. Sturm, L. D., Williams, C. B., Camelio, J. A., White, J., Parker, R. Cyberphysical vulnerabilities in additive manufacturing systems: A case study attack on the. stl le with human subjects, Journal of Manufacturing Systems 44 (2017) 154-164

39. Pope, G., Yampolskiy, M., A Hazard Analysis Technique for Additive Manufacturing,in: Better Software East Conference, 2016, p. 17. URL http://arxiv.org/abs/1706.00497

40. Gupta, N, Tiwari Akash, Satish T. S. Bukkapatnam and Ramesh Karri, (Fellow, IEEE), Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks, (Fellow, IEEE)

41. Kovacs, E. (2018). Thousands of 3D Printers Exposed to Remote Attacks. Retrieved from https:// www.securityweek.com/ thousands-3d-printers-exposed-remote-attacks printers open to internet direct attacks.

42. Chen, F., Mac, G. and Gupta, N. ``Security features embedded in computer aided design (CAD) solid models for additive manufacturing,'' Mater. Des., vol. 128, pp. 182194, Aug. 2017.

43. Sapkota, A. (2020). 3D Bioprinting- Definition, Principle, Process, Types, Applications. Retrieved from https://microbenotes.com/ category/biotechnology/

44. Ghadge, A., Dani, S., Chester, M. and Kalawsky, R.``A systems approach for modelling supply chain risks,'' Supply Chain Manage., Int. J., vol. 18, no. 5, pp. 523538, Jul. 2013.

45. Maxwell, K., Microsoft. (2021). How Microsoft is Driving Defense Innovation at the Speed of Relevance. Digital Report 2021, 2-3.

46. GE Additive, (2021). 3D Printing in the Oil and Gas Industry. Additive Manufacturing. Retrieved from https://www.ge.com/additive/ additive-manufacturing/industries/oil-gas

47. Department of Defence, (2021). Department of Defense Additive Manufacturing Strategy Retrieved from https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing- strategy.pdf

List of Figures

Figure 1: 3D Printing in a desert deployment zone [7]

Figure 2: 3D Printed Grenade Launcher [18]

Figure 3: The impact of induced defects in critical components in the dr0wned study [22]

Figure 4: Examples of critical defects inserted maliciously into a design

Figure 5: Internal testing with a critical defect in the arm once printed and assembled

Figure 6: Education, healthcare, and finance have a higher percentage of breaches compared to their percent of the GDP. However, the focus of this paper is on the manufacturing industry with the highest GDP percentage[1]. Image credit Council of Economic Advisers 2018

Figure 7: The percentage of negative cumulative abnormal returns for a given category of cybersecurity breach. Market perception of company value, as a result of IP theft, is a 36% more damaging category than the next highest. The severity of the abnormal drop in market returns gives the score credence. Cybercrime is on the rise, and IP is a very costly target.[1] Image credit Council of Economic Advisers 2018

Figure 8: Attacks in the design stage in the supply chain of AM components [40]

Figure 9: Attacks on raw materials in the supply chain of AM components [40]

Figure 10: Attacks on printer hardware in the supply chain of AM components [40]

Figure 11: DEFEND3D Software. End-to-end encryption securely delivering virtual inventory

Glossary

Additive Manufacturing (AM)	An industrial production process controlled by a computer that creates three dimensional objects by depositing materials, usually in layers.
AM Sabotage	Referred to Additive Manufacturing, the act of doing deliberate damage to equipment, digital files, machines, etc. to prevent an adversary from using them.
Application Programmable Interface (API)	A set of functions and procedures allowing the transport of data between two applications.
Biological Additive Manufacturing (Bio AM)/Bioprinting	Comprises of the use of 3D printing technology with materials that incorporate viable living cells such as producing tissue for reconstructive surgery or replacement organs.
Blockchain	Blockchain is a database that stores encrypted blocks of data, then chains them together to form a chronological single-source-of-truth for the data.
CAD	Computer-Aided Design.
Containerization	A form of operating system virtualization, through which applications are run in isolated user spaces called containers, all using the same shared operating system (OS). A container is essentially a fully packaged and portable computing environment.
CT Scan	An X-ray image made using a form of tomography in which a computer controls the motion of the X-ray source and detectors, processes the data, and produces the image.
Cybercrime	Criminal activities carried out by means of computers or the internet.
Digital Asset	Anything that exists in a digital format and comes with the right to use.
Digital Thread	The digital thread consists of a communication framework that helps in facilitating an integrated view and connected data flow of the product's data throughout its lifecycle.

Field Programmable Gate Array (FPGA)

A chip that has its internal logic circuits programmed by the customer.

Finite Element Analysis (FEA)

Simulating the behavior of a part or assembly under given conditions so that it can be assessed using numerically differential equations solutions.

G-code

Computer numerical control programming language.

Human mesenchymal stem/stromal cells (hMSCs)

Human stromal (mesenchymal) stem cells represent a group of non-hematopoietic stem cells present in the bone marrow stroma and the stroma of other organs including subcutaneous adipose tissue, and muscles.

Infrastructure as a Service (IaaS)

An online service that provides physical computing resources, location, data partitioning, scaling, security, backup etc.

Industrial Espionage

Illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage.

Industry 4.0 (IR 4.0)

The Fourth Industrial Revolution is the ongoing automation of traditional manufacturing and industrial practices, using modern technology and IoT.

Inverse Graphics GAN

Generating 3D Shapes from unstructured 2D data.

IoT

The Internet of Things describes the network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

Intellectual Property (IP)

Creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

IP Theft

Any act related to the illegal appropriation of ideas, inventions, and creative expressions such as trade secrets and proprietary products.

Key Performance Indicator (KPI)

A measurable value that demonstrates how effectively a company is achieving key business objectives.

Machine Learning (ML)

The capacity of a computer to process and evaluate data beyond programmed algorithms, through contextualized inference.

Platform as a Service (PaaS)

A cloud computing model where a third-party provider delivers hardware and software tools to users over the internet.

Reverse Engineering

The reproduction of another manufacturer's product following detailed examination of its construction or composition.

Serverless Computing

Serverless computing enables developers to build applications faster by eliminating the need for them to manage infrastructure.

SDK

Software development kit.

Stack

Localized cloud recreating the cloud experience in a closed, off-line environment.

Sustainment

Sustainment is the provision of logistics, financial management, personnel services, and health service support necessary to maintain operations until successful mission completion.

Systems Theoretic Process Analysis (STPA)

Hazard analysis technique based on STAMP, Systems-Theoretic Accident Model and Processes. It is an accident causation model based on systems theory and systems thinking.

Virtual Machine (VM)

A physical computer resource that is contained within the cloud.

Virtual Private Network (VPN)

An encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

Imperial College London
Institute for Security Science and Technology (ISST)
Imperial College Business School
80 Wood Lane
London
W12 7TA
United Kingdom

info@defend3d.com

Document Layout
Reza Ali

Image Editing
Miguel Sousa


DEFENDED