ORIGINAL RESEARCH
published: 16 November 2021
doi: 10.3389/feduc.2021.768037

Modelling Cyberspace to Determine Cybersecurity Training Requirements

Adrian Venables *

Department of Software Science, Tallinn University of Technology, Tallinn, Estonia

Cyberspace is a constantly evolving and expanding environment that is being used for an ever-increasing range of purposes. As such, it attracts numerous threat actors seeking to identify and exploit its vulnerabilities. In order to be able to fully mitigate the risk of compromise, it is necessary to first understand the nature and composition of cyberspace and how it is used. This chapter seeks to address this issue by presenting a method to model cyberspace in three dimensions with humans included as an integral part. Expanding beyond describing cyberspace purely in terms of technology and its uses, it explores geographic, political, and temporal aspects to reflect its dynamic nature. The first component of the model examines the varied attributes of cyberspace ranging from the landscape in which its components are located to how they are used. The second dimension investigates the path of data in all its forms from its source to destination, emphasising that cyberspace is fundamentally a communications medium and is not borderless. Thirdly, it focuses on the security dimension and the motivations of those with malicious intent, demonstrating the multidisciplinary and essentially human nature of cybersecurity in countering their activities.

Keywords: cyberspace, cybersecurity, cyber operations, threat modelling, cybersecurity training, cyber situational awareness

OPEN ACCESS

Edited by:
Benjamin James Knox,
Norwegian University of Science and Technology, Norway

Reviewed by:
Mazaher Kianpour,
Norwegian University of Science and Technology, Norway
Kirsi Helkala,
Norwegian Defence University College, Norway

****Correspondence:***
Adrian Venables
adrian.venables@taltech.ee

Specialty section:
This article was submitted to Higher Education, a section of the journal Frontiers in Education

Received: *31 August 2021*
Accepted: *01 October 2021*
Published: *16 November 2021*

Citation:
Venables A (2021) Modelling Cyberspace to Determine Cybersecurity Training Requirements. Front. Educ. 6:768037. doi: 10.3389/feduc.2021.768037

INTRODUCTION

The role of cybersecurity is well understood and has become the basis for a thriving and successful industry. Supporting this profession is a mature and fully developed education and training organisation providing the range of skillsets needed to supply suitably qualified personnel. However, the complexity of the discipline is such that individuals tend not to be aware of all aspects of the subject. This can lead to cybersecurity practitioners concentrating on just those niche areas in which they have been trained resulting in a very narrow view of the profession. The challenge of end-to-end security encompassing all aspects of cyberspace is rarely considered and for good reason. As an artificial environment that is constantly expanding with new uses being found and novel technologies continually introduced, achieving total security is a formidable undertaking. Indeed, it may be considered so large and complex as to be disregarded as impracticable. This chapter seeks to address this issue by presenting a novel way of representing cyberspace to enable all aspects to be examined. Drawing on previous research, it introduces a three-dimensional model of the environment optimised to better understand how its properties, attributes, and risks can be understood at any place and time. In doing so, it demonstrates that cyberspace does not exhibit universal characteristics but that its structure and characteristics may differ at the source and destination of any data exchange. By achieving a greater appreciation of the properties of that part of cyberspace relevant to a particular use case, the training required to provide comprehensive cybersecurity can be better understood.

DEFINING CYBERSPACE

Before considering how to secure cyberspace, it is necessary to understand and define its composition, and this presents the first challenge. Such is the complexity of the environment and the multitude of technologies and uses for which it is employed that there is no common agreement on a definition. Multiple descriptions have been proposed, each differing depending on what electronic components are utilised, and how they are used. This lack of consensus on a definitive description of what constitutes cyberspace was illustrated as far back as 2009 with Franklin D Kramer identifying 28 different definitions of the term (Kramer, 2009, 4). Eight years later, the NATO affiliated Cooperative Cyber Defence Centre of Excellence (CCD COE) collected 29 descriptions of cyberspace from a range of agencies and countries. Although there were similarities in some explanations, others were very different (Bigelow, 2018, 123–138). The Oxford English Dictionary offers the following rather esoteric explanation based on the provenance of the word from William Gibson's (1994) science fiction novel Neuromancer. This cyberpunk classic originally described cyberspace as a "consensual hallucination" (Gibson, 1994, 3).

> The space of virtual reality; the notional environment within which electronic communication (esp. *via* the Internet) occurs (Oxford English Dictionary, 2021).

NATO acknowledged cyberspace as a domain of operations in 2016 (NATO HQ, 2021). However, it was only in 2019 that it first provided an entry in their glossary of terms and definitions. This stated that cyberspace was:

> The global domain consisting of all interconnected communication, information technology, and other electronic systems, networks, and their data, including those which are separated or independent, which process, store, or transmit data (NATO Standardization Office, 2020, 37).

Accepting that this agreed definition was a significant step for the alliance, this characterisation of cyberspace is very narrow and focuses on technology at the expense of other important attributes. It does have its uses though as it underpins the foundation for defining the future military response to cyber threats and inform the training required to counter them. It can also provide an effective foundation on which to advance theory and practice in developing new ways to exploit its attributes to achieve both strategic and tactical advantage. Trying to develop consistent tactics, techniques, and procedures (TTPs) for cyber operations without an agreed definition of what the environment comprises is a challenging prospect. Similarly, planning operations to achieve military effects in cyberspace cannot be realistically achieved without agreement of where they are to be directed or what the impact will be. It is of note that the other domains of warfare, land, air, sea, and space, already have clear definitions of what they are and how they are bounded. As for other operations, military cyber activity is also subject to legal oversight, and without an "official" definition, lawyers would have difficulty being able to approve offensive cyber actions.

Although there are some benefits to precisely defining cyberspace, its unique attributes mean that there are some distinct advantages to not having a universally agreed meaning. Not being constrained to a single description provides flexibility to describe it in terms to suit a particular purpose and to adapt as technology develops and requirements evolve. As policy and funding decisions may be justified based on recognised terms, seeking approval for novel projects may be challenging if they do not fit a standard framework. New uses may also emerge that are outside the scope of the term. The NATO definition, for example, does not encompass the cyber-physical environment encompassing the "Internet of Things" in which connected devices are able to cause a change to its surroundings. For NATO and other military organisations, rapid doctrinal development may also be hindered as terms become obsolescent and outdated. Adversaries that may not be so constrained by working within the bounds of policy publications may be more agile, and the flexibility to counter their tactics may be hindered. Finally, not having a recognised definition can encourage a more free-thinking environment and will encourage innovative thinking. Creating artificial barriers between disciplines can stifle the creation and exploitation of new ideas and innovative thinking.

The difficulty of producing a succinct, yet comprehensive and universally accepted, and enduring definition of cyberspace aptly demonstrates its unique characteristics of malleability, flexibility, and continuing evolving nature. Attempts that so far have been made to describe cyberspace have either been incomplete or highlight a single or narrow range of attributes. This failure to encompass its full potential limits thinking and results in an inability to represent the full range of uses for which it can be exploited. Instead, some definitions lead to the environment being viewed from within the context of achieving a particular aim with descriptions developed solely for that purpose. This chapter continues the tradition of attempting to explain cyberspace but differs by offering a method by which comprehensive training requirements can be identified and developed. Comprising four sections, it builds on previously published literature to present a new model of cyberspace optimised to explain the relationship between the physical world, technology, and human users. A key aspect of this description is that it emphasises that cyberspace can be modelled in three dimensions. This accounts for its attributes differing at the location from which information originates, where it transits, and at its destination. Thus, the nature of cyberspace at the point where a target audience accesses information is just as important in terms of security as the location of the originator. In the first section, earlier work to characterise and define cyberspace in terms of a number of vertical layers is examined. This demonstrates how attempts to explain this man-made environment have evolved and developed. Secondly, these earlier models are expanded to include new aspects not previously considered but are considered fundamental to understanding the cyber environment and the skills needed to secure it. Thirdly, a second dimension is introduced to present a notion of distance to cyberspace. This is significant as the often-instantaneous nature of communication through networks and the opaque nature of its routing are often disregarded as a significant factor in its security. This section explores the significance of the lack of control over the path that data follow as it may be subject to filtering, censorship, or other forms of interference. Under these circumstances, knowledge of this route becomes a significant issue, and there is utility in appreciating the distance and path it follows. Finally, the inclusion of a third dimension to the model of cyberspace considers the range of security threats and how risks can be mitigated. This is important as it demonstrates that cybersecurity training requirements may need to accommodate a wide range of factors. These depend on a thorough understanding of the risk, which differ depending on how cyberspace is used and that it is not just one big network with similar properties throughout.

ATTRIBUTES OF CYBERSPACE

A Brief History of Cyberspace

Although any definition of cyberspace is open to interpretation depending upon the technology employed and its use, its origin is well documented. Originally funded by the U.S. Department of Defense, the Advanced Research Projects Agency Network or ARPANET was invented in the late 1960s (Leiner et al., 1997). Its purpose was to allow computers in geographically separated universities to communicate on a single network. The term "Internet" was first coined in 1974 to describe a single global network by pioneering computer scientist Vint Cerf. However, it was not until 1983 when all computers on the ARPANET switched to a single communications protocol that its use expanded and became more widely accessible (Brady and Elkner, 2017). Unfortunately, in these halcyon early days, security was not a design priority for the early Internet pioneers. They were constrained by the technology of the time and could never have foreseen the ways in which their technology would be harnessed in the future. This resulted in a fundamentally insecure network that was open to abuse by those with malicious intent. Following a series of incidents in which the attributes of the Internet were abused to varying degrees, the cybersecurity industry evolved dedicated to developing ways to protect it (Townsend, n.d.).

As a communications medium, cyberspace can provide global access to resources in a range of formats that have been invented to meet the requirements of its users. Time and distance have been collapsed with the instantaneous retrieval of information possible from creators worldwide. With its origin in the hippy culture of California in the 1960s, there was an aspiration that this new network would be considered as a "Global Commons." International law identifies four Global Commons: The High Seas, the Atmosphere, Antarctica, and Outer Space. These are areas that have been traditionally defined as those parts of the planet that fall outside national jurisdictions and to which all nations have access (UN System Task Team, 2013). With the development of cyberspace and its increasing importance to the functioning of society, it has been suggested that it too be added to this list (Stang, 2013). This idealist thinking is however naive and fails to understand the composition and functioning of the medium. Every aspect of cyberspace is owned and maintained and must therefore generate income to be sustainable. This may be invisible to the user, but cost models exist that enable the infrastructure to function. Ownership implies control and so authority over the right of admission. This can extend to preventing certain groups of users, data formats, or information originating from a specific location from accessing the network. The economic realities of maintaining an artificial environment were first exposed in February 1976 in an open letter written by Bill Gates to computer hobbyists. In it, he opposed the popular view that hardware must be bought but the software was considered free and openly shared among users. By explaining that the popular BASIC operating system that he had commissioned had cost money to produce, he complained that fewer than 10% of users had actually paid for it (Gates, 1976). This disincentivised the production of further software upon which the hobbyists relied. At the time, the letter was highly controversial as it openly accused those who shared software of theft. However, Gate's letter exposing the issues subsequently laid the foundation for the software industry upon which the functioning of cyberspace relies.

Accessing Cyberspace

Although users can access Internet resources globally, there is the misapprehension that cyberspace is borderless. However, this could not be further from the truth. The subject of Internet censorship that restricts the flow of information was researched from 2004 to 2014 by the OpenNet Initiative (ONI), a collaborative partnership of three US and Canadian Institutions (OpenNet Initiative, 2014). Their aim was to investigate, expose, and analyse what they believed to be the increasing amount of filtering and censorship of Internet content in a credible and nonpartisan fashion. The ONI concluded that over three dozen states, clustered mainly in East Asia, the Middle East, North Africa, and central Asia, were actively filtering Internet traffic. Of these, China had the most extensive filtering regime in the world. The so-called "Great Firewall of China" is renowned for blocking access to internationally popular and commonly used sites. These include business-focused sites, email, social media, streaming, news, search engines, messaging, blogging, video communication, adult material, and politically sensitive pages (Travel China Cheaper, 2021). The ONI also noted that content was blocked within the US and Europe. Restricted subjects including material related to extreme pornography or imagery related to Nazism or holocaust denial. The ONI concluded that online censorship was becoming increasingly important to countries seeking to curb dissent, with the main topics filtered related to political, social, and security issues. They also identified a fourth theme that of the use of Internet tools. This included networking applications designed to allow the sharing of information, translation of websites, anonymisers, blogging, or Voice over Internet Protocol (VoIP) services. Furthermore, social media, which is one of the key methods of communication at a peer-to-peer level, was recognised by the ONI as a particularly popular subject for censorship.

The unique properties of cyberspace present unique security challenges for both civilian and military users. Indeed, the vital role played by security professionals has been particularly acknowledged by the military now that cyberspace is recognised as being of equal importance to the other warfighting domains. The primary reason why security is of such concern is that the cost of entry for potential threat actors is very low. All that is required is a network-enabled device and an Internet connection. Both are straightforward to access and with the increasing prevalence of wireless hotspots may even be free. This, combined with the ease by which knowledge can be obtained, has resulted in a range of nascent attackers with varying degrees of competence. Gaining the ability to write malicious code is not difficult with books, online tutorials, and industry courses readily available. For those that do not have the motivation to write their own code, there are many freely available tools online that can be accessed. This includes a ready-made free operating system containing a complete set of applications to attack target systems with low to medium levels of protection (Offensive Security, 2021). This has resulted in an asymmetric effect in which poorly funded, small groups with limited skills and resources can achieve an impact disproportionate to their size. An example of this was the infamous compromise of the UK telecommunications provider TalkTalk in 2015. Two self-taught teenagers were able to use a simple technique to access the details of 157,000 customers costing the company an estimated £60 million pounds (IT Pro, 2017). At the state level, countries can also exert an effect disproportionate to their size. In 2018, US prosecutors sought to indict a North Korean national accused of leading a series of financially and politically motivated cyber-attacks. Although economically weak and with limited global influence, North Korea is a significant global cyber power and has been accused of a range of bold campaigns. These included operations to obtain foreign currency through the theft of assets from a bank in Bangladesh and the creation of a Ransomware campaign (US-CERT, 2020, 1). However, perhaps the most significant was the attack on Sony in 2014 in response to a film that featured the North Korean leader (Starks, 2018). This sophisticated operation exfiltrated commercially sensitive data and deleted the contents of a significant proportion of Sony's internal network, almost causing the company to collapse (Peters, 2014). Its impact, combined with threats to cinemas that were planning on showing the film, achieved the aim of preventing its widespread release.

The ease of access to cyberspace and the range of hacking tools available, combined with the inherent insecurity of the Internet, mean that attacks will always be easier than defence. Computer hackers have obtained a cult-like status as being the most skilled and respected within the online community. However, it can be argued that the defenders are the unsung heroes of the industry. Computer software is complex and must work with numerous other applications. Cyberspace is constantly evolving, developing, advancing, and expanding, with each new software application and update exposing new vulnerabilities that once found can be exploited. Attackers only need to be lucky once to gain access to a system. Defenders must be constantly vigilant against a constantly changing landscape with the potential that a single breach of their systems can be catastrophic. As well as countering potentially vulnerable hardware and software, defenders also must consider new technologies that expose additional access points. The so-called Internet-connected "smart" devices and a trend to join ever more previously unconnected technologies to the Internet increase the attack surface. This "Internet of Things" includes wearable devices that constantly collect personal data leading to ever more attractive targets for those with malicious intent.

The Militarisation of Cyberspace

As with the physical environments, cyberspace has become militarised. However, as a domain of warfare, it has unique characteristics that must be considered when modelling its attributes. Firstly, cyberspace is artificial. Wars can be fought on land, sea, air, and space; but after the battle is over, the field of conflict remains. This is not so of cyberspace that can be created, altered, or destroyed in addition to needing continual maintenance to function. Secondly, its role has become crucial to the way that conflict is undertaken. Military capabilities across the other domains are increasingly being managed through cyberspace, and armed forces are finding it ever more challenging to operate in a cyber-denied environment. Thirdly, military cyber operations also do not just concern the armed forces but can affect non-combatants in a way not seen in other forms of warfare. Military and Civilian use of the same infrastructure, and networks and software applications have become the norm. Their use is so intertwined that it is difficult to differentiate between them. Denying the use of certain networks used by a hostile force can potentially affect their civilian infrastructure to such an extent that it could be regarded as a war crime. Naturally, this would not be an issue to some potential adversaries, but it does emphasise the need for the highest standard of protection to be applied to all networks. This places an increasing burden on cybersecurity specialists who may find themselves counting military adversaries as well as civilian attackers.

Cyberspace has become the preferred environment for states to engage in hostile activities that if undertaken in the physical environments may invoke a military response. Effects can be achieved that are similar in result to the destructive capabilities of conventional munitions. Such examples include the Stuxnet worm against the Iranian nuclear programme and the Not Petya attacks that were focused on organisations using Ukrainian tax accounting software. However, it can also be used for other purposes. As well as achieving permanent damage on a target, it can be used to deliver temporary effects when desired. This can degrade systems that it may be preferable to be maintained such as electrical or communications networks. Offensive cyber operations can also be used for espionage purposes to extract data or to target users by subverting their beliefs or for deception. As well as being flexible and versatile, cyber operations also present another powerful feature—the difficulty of attribution. Under international law, military forces are required to identify themselves; hence, soldiers wear uniform, warships fly flags, and military aircraft have national markings (ICRC, 2021). Malicious code in cyberspace is more difficult to identify as nations' military forces, terrorist groups, criminals with a range of motivations, and amateur hackers can all use similar techniques. Bespoke cyberweapons can contain no clear identity of its origin, and the method by which the attacks are routed from source to destination can be disguised. Hostile entities can take deliberate measures to suggest that their attacks have originated from elsewhere and can repurpose code used by others. Although the source of a sophisticated attack can be strongly suspected, achieving attribution is a complex, expensive, and time-consuming process. For example, although North Korea was quickly suspected as the perpetrator of the Sony attacks, it took the US authorities 4 years to identify the individuals responsible (FBI, 2014). This was too long for any meaningful military response to be effective but did result in sanctions against the country (US Department of Justice, 2018). Using the attributes of cyberspace to achieve military objectives without crossing the threshold of the legal definition of hostile action has led to a range of new terms. These include "lawfare," "hybrid operations," and the "grey zone" of warfare, which are increasingly being used by a range of nations (Lawfare, 2021). Attempts have been made to study how international law can be applied to cyber operations with the most prominent being the "Tallinn Manual" (Schmitt, 2013). This non-binding academic analysis was produced by a group of international experts who sought to interpret international law in the context of cyber operations and cyber warfare. However, without a formal legal agreement, cyberspace remains attractive for offensive activity and a challenging environment to defend, which highlights the importance of a robust and comprehensive approach to security.

MODELLING CYBERSPACE—THE FIRST DIMENSION

As we have seen, cyberspace is a dynamic and complex environment, and this makes the prospect of securing it a challenging undertaking. It has been said that "If You Can't Measure It, You Can't Improve It," and this can be applied to cybersecurity (Katzman, 2016, 23). To be able to effectively protect something, it is necessary to be able to bound it, understand its composition and appreciate where the vulnerabilities are. The rest of this chapter will be devoted to presenting a method of modelling cyberspace to better understand its composition, properties, risks, threats, and therefore its security requirements. To do so, a three-dimensional model will be presented consisting of layers, each with unique properties and attributes. A key concept is that the attributes are not universal but differ throughout. Thus, the properties and vulnerabilities at one point will be different at another, and this model will assist in understanding and appreciating these variances. Viewing cyberspace in this way will also help to dispel the unhelpful notion of cyberspace as a "cloud," which has become a popular term. Any data stored or processed "in the cloud" purely means that it is located on somebody else's computer and accessed remotely. Although this can be useful for delegating responsibility for backups and having efficient storage and processing capacity, ultimately data still reside on physical hardware somewhere. Being able to recognise the path between you and your data is therefore important to ensure resilience and being able to access it when required. This model provides an explanation of what cyberspace is and what it can be used for. This can contribute to what can be termed "situational awareness." This is a military term defined as the knowledge of the elements in the battlespace necessary to make well-informed decisions (NATO Standardization Office, 2020, 119). Good cyber situational awareness can provide the necessary information to make informed security decisions, and a method to model cyberspace can provide a means to understand the environment.

Writing for the RAND Corporation in 2009, Martin Libicki acknowledged that as a virtual medium, cyberspace is much less tangible than the other physical environments of land, sea, air, or space (Libicki, 2009, 12). In describing its nature, he viewed it as consisting of three layers: physical, Syntactic, and Semantic. Together, these describe the core elements of its composition, but not its use or how they can be applied in any single context. He defined the physical layer as being the hardware components and wires, which together form the part of cyberspace that is susceptible to kinetic attack and physical destruction. The Syntactic layer sits above the physical and contains the code and protocols. This enables the components of the physical layer to interact with each other and includes such functions as device recognition, addressing, and routing. The complexity of the Syntactic layer is dependent upon the type of system in use and will be bespoke to the user requirement. It is the layer that would be targeted remotely across the network by hackers seeking to access or manipulate the software without having physical access to the hardware. At the top of Libicki's stack is the Semantic layer, which contains information that makes the totality of the system useful to the operator. This includes files such as address lookup tables and process control information that are user-provided and enable the system to perform as intended. John Sheldon also described cyberspace in terms of layers but increased the number to four and emphasised that control of one layer does not mean control of the others (Sheldon, 2011, 98). Again, the infrastructure at the base of the stack contains the material components such as hardware and cabling, but above it is a physical layer. This considers the properties of the electromagnetic spectrum that animate the infrastructure layer. This is an important consideration as it highlights that cyberspace is not uniform and draws on a range of methods and media to transmit information from source to destination. Above the physical layer is the Syntactic layer containing data formatting information and the protocols that control cyberspace. Finally, at the top level is the Semantic layer that makes information useful and comprehensible to users. Sheldon notes that when attacking a system, the layer targeted depends on what outcome is trying to be achieved. For example, stopping a system from working will involve the Syntactic and

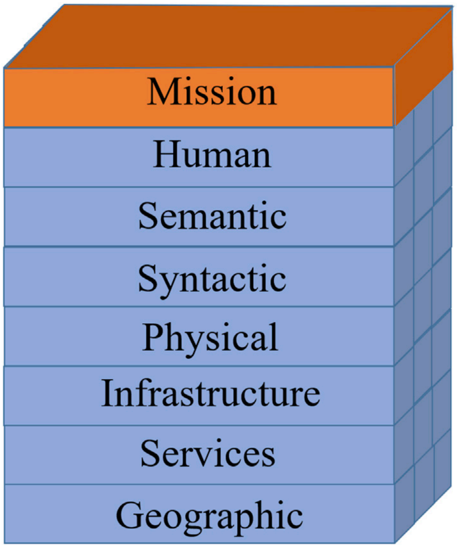

FIGURE 1 | The eight-layer model of cyberspace.

infrastructure layers, whereas spoofing a user will involve manipulation of the Semantic layer.

Comparing the evolution of these previous models with the new model described here demonstrates how the perspective of cyberspace has changed with advances in technology and use. Initially, in his three-layer model of physical, Syntactic, and Semantic layers, Libicki described the environment in technical terms, but not how it could be utilised. He did not consider variations in its composition or how it is reliant on external factors. His view described it as essentially a network within which computer code enables the transfer of information. Sheldon, however, does appreciate the layers as having their own very distinct characteristics and that the lowest, infrastructure layer is more complex than just consisting of hardware and wires. His physical layer, which considers the electromagnetic properties of the infrastructure layer, acknowledges that the communication method may have a bearing on the success of its receipt. However, neither considers how cyberspace may be employed for any single purpose or how its existence depends on the physical environment or the human user for its existence and security.

The previous purely technical perspective of cyberspace and lack of human involvement are considered in the “Society 5.0” initiative that originated from a Japanese government programme. This defines a human-centred society that balances economic advancement with the resolution of social problems by a system that integrates cyberspace and physical space (Society 5.0, 2021). It follows Society 1.0—hunting and gathering, Society 2.0—agricultural society, Society 3.0—industrial society, and Society 4.0—information society (Cabinet office of Japan, 2021). Society 5.0 describes how people, devices, and systems are connected in cyberspace and how artificial intelligence can influence the physical space. However, whereas it describes an end state, it does not seek to explore in detail the technical requirements or address security issues. To address the shortcomings in these previous depictions of cyberspace, the following model expands and develops these previous works. It comprises eight layers and adds two further dimensions to provide a comprehensive model of cyberspace and the threats to the information it contains. The eight-layer model is shown in **Figure 1** below and is followed by a detailed explanation of each component.

Geographic Layer

The first layer of cyberspace to be considered is at the bottom of the stack and is termed Geographic. This emphasises the real-world environment in which the infrastructure and users reside and where that part of cyberspace to be protected is located. Geography is significant when considering the other properties and attributes of cyberspace. For example, propagation by air or space can only be by radiofrequency (RF) transmission, whereas at sea, it may be *via* undersea cable or wirelessly between vessels or with the shore. On land, depending on location, it might be either wired or wireless as regional variations in the terrain are significant. Shifting desert sands may prevent the use of mast-mounted microwave links, and mountainous regions may not favour buried cables. Political aspects may also need to be considered in this layer as some countries may not allow free passage of data across their borders without monitoring or censorship. Some nations may also not have invested in a widespread modern infrastructure resulting in the speed of transmission within their borders being limited. As the means by which networks are formed and their propagation characteristics are fundamental to the properties of cyberspace, understanding the geographic area is vital when considering security. It may be relevant that the route taken may influence the type of message that can be transmitted as some formats such as encrypted traffic may be restricted in certain areas. Also, a congested or legacy network may not have sufficient bandwidth capacity to transmit data-hungry services such as high-definition multimedia. As the requirements of users increase and capacity becomes insufficient to meet demand, they may become increasingly vulnerable to denial-of-service attacks intended to overload networks.

Services Layer

Sitting above the geographic layer are the elements that must be present to enable cyberspace to exist. These are what have been termed “cyberspace littorals,” which are the places where cyberspace and the other environments meet (Withers, 2015, 126–150). Included in this description are utilities such as power supplies, chilled water, air conditioning, and even the security of the buildings housing computers, servers, and networking components. Although these are not normally regarded as integral components of cyberspace, they emphasise its fragility and reliance upon external factors for it to function correctly. This is highlighted in that not only do all electronic components require a reliable and stable power supply but also they in turn generate heat. This in turn requires additional power to be generated and supplied to cool them (Balandin, 2009, 34–39). It should also be remembered that the Internet was not originally designed to accommodate the level of expansion and growth that has since materialised. This has resulted in some critical locations becoming hubs for regional connectivity and so single points of failure. There is the very real possibility that should the Services layer be compromised at these sites it could result in the disconnection of whole urban areas (Strassmann, 2009). Security considerations of the Services layer would include an appreciation of a country's capability to support its critical national infrastructure (CNI). These are the utilities required to maintain its cyber framework including the ability to attract and train the skilled personnel necessary to ensure its continued operation. Crime rates, particularly when considering component theft, could also be included in an overall assessment of the resilience of the Services layer. In terms of vulnerabilities, it may be that this layer is the most attractive to an adversary. This may be due to it being at the greatest exposure to physical attack and that the aftereffects may be clearly obvious to observe and assess. Brute force destruction may also be easier than the effort involved in writing a malware payload to achieve a similar effect. This vulnerability may be compounded by third-party organisations such as utility companies having a contracted availability criterion of less than 100% and regard some level of failure as acceptable. Some components of the Services layer such as electrical substations may also be outside the protective perimeter of an area containing the more obvious elements of the cyber infrastructure. These will be more challenging to monitor and protect but are as much a consideration of cyber security as other more commonly considered aspects. Attacking power supplies to degrade a country's infrastructure has already been recognised by America's development of the so-called "CBU-94 Blackout Bomb" first used in 1999 against Serbia. This munition consisted of a bomb that dispenses chemically treated carbon graphite filaments. These short-circuit electrical power distribution equipment such as transformers and switching stations to mitigate the risk of collateral damage that may be caused by conventional weapons (Global Security, 2011). Attacking electricity generation was also an objective of Russia's Sandworm group in Ukraine that successfully, albeit temporarily left 230,000 without power (Greenberg, 2019, 50–58).

Infrastructure Layer

This comprises the physical embodiment of cyberspace and incorporates the hardware components that collect, store, process, communicate, present, and transfer data. This layer includes computer clients, servers, industrial control systems, networking components, cabling, microwave towers, satellites and ground stations, and other elements fundamental to the operation of cyberspace. Whereas the Services layer provides the supporting function to cyberspace but carries no data itself, the Infrastructure layer is defined as all the components through which information passes. These include the end points, connecting nodes, and all points in between. The Infrastructure layer is also the most widely dispersed element of cyberspace as it comprises the different types of cabling through which most domestic and international communication passes. It also includes the devices that users interact with such as personal computers, laptops, tablets, smart phones, wearable devices, and medical implants as well as their associated wireless connectivity. An important consideration of the Infrastructure layer is that every component is owned and therefore under the authority of an organisation. Ownership can range from governments, international and national commercial enterprises controlling large network infrastructures to individuals and their personal devices. As nations have ultimate authority over the Infrastructure layer within their borders, their governments have complete control of its availability and how content can be filtered, censored, or prioritised. Of increasing significance is also how this aspect of cyberspace is also increasingly owned by the content providers themselves. This is the case with Google Fiber, which is being installed in some cities in the US with promised speeds of up to 1,000 megabits per second (MBPS). It will be aligned to the company's other services such as Google Drive's cloud storage facility and its television service Google Cast (Google, 2021). However, not all infrastructure projects are so successful. In early 2021, Google's parent firm Alphabet announced that it was shutting down Loon. This was an ambitious project that sought to connect those areas that did not have Internet access using balloons floating in the stratosphere to provide wireless cellular access. The reason given was that it was unable to find a sustainable business model and partners despite raising $125 of investment in 2019 (Singh, 2021). Such decisions highlight the infrastructure challenges of connecting unserved and underserved communities around the world that may not be profitable in the short or immediate term.

As for the Services layer, the security of the Infrastructure layer is primarily that of protecting components. This layer is susceptible to kinetic attack with theft or physical destruction of components a significant threat, with their replacement and installation imposing cost and taking time to complete. If access to the equipment is possible, physical destruction is also the easiest for threat actors to undertake due to the complexity and fragility of electronic systems. Importantly, this layer also includes connected industrial complexes and their networked machinery components. Instead of being designed to transfer data externally to other locations, these act as their own end points to control and manage electro-mechanical systems internally. Security of these systems is paramount as a compromise here could lead to adverse physical effects. If damaged, it may take some time to repair if specialist components are not easily acquired due to complexity, location, or other demands on production. Cost of replacement may also be an issue if they are particularly expensive, and it may take time to release the required funds to the manufacturing company.

Physical Layer

In his 2009 model of cyberspace, Libicki describes his Physical layer as being the hardware components and wires (Libicki, 2009, 12). Together, these form that part of cyberspace that is susceptible to kinetic attack and physical destruction. Sheldon calls this as the Infrastructure layer, a term used in this model, and presents a new definition for the Physical layer (Sheldon, 2011, 98). This introduces the role of the electromagnetic spectrum in describing the properties of cyberspace and incorporates features that are governed by the laws of physics. These describe the properties and techniques that animate the Infrastructure layer and enable data to be exchanged between systems. This is an important consideration as it highlights that cyberspace is not uniform and draws on a range of methods and media to transmit information from source to destination. In wired connections, these comprise the passage of photons in fibre-optic cables and electrons in cabling. In wireless communications, a wide range of frequencies are utilised in a variety of systems including mobile telephony, Wi-Fi, Bluetooth, point-to-point microwave, and international satellite links. The Physical layer determines the characteristics of cyberspace in a distinct region as data transfer rates vary considerably depending on the medium of transmission and the frequency and power used. Furthermore, speed may also be an issue as although faster than copper wiring, transmission through fibre-optic cable is slower than a microwave link. This is because energy travels quicker through air than through glass, which in turn is faster than metal. This may not be an issue for most users, but within the financial industry, it is an important consideration. To serve the requirements of high-speed automated trading where knowing commodity prices, a millisecond advantage in transmission times can make the difference in securing a profit (Blum, 2012, 47).

In addition to the propagation properties of the transmitted frequency used by each technology, the range may also be restricted by licensing agreements limiting the power that can be used. The RF spectrum is a congested environment with frequency bands used for multiple purposes and so is strictly regulated nationally and internationally. However, many frequency bands are not under the control of any one authority and are used for multiple purposes. For example, the ultra-high frequency (UHF) band from 300 to 3,000 MHz may be used for both non-communications as well as communications transmission. The former includes long-range air traffic and weather radar, key fobs, and microwave ovens. For communications, mobile telephony, microwave communications, Wi-Fi, Bluetooth, satellite communications, satellite navigation, and voice communications also use this band. Restricting the range, using shielding, time-sharing, and employing directional transmissions can enable multiple users to access the same spectrum without mutual interference.

Security of the Physical layer is dependent upon the components used, and the method of transmission employed. Wired installations have the same vulnerabilities as the Infrastructure layer and may be sabotaged by cutting or tapping to intercept or insert data. Shielding, burying, or other physical methods of protection can provide security with the use of additional cables in different routes providing resilience. Wireless communications are vulnerable to attack their transmitters but are generally more susceptible to non-kinetic methods. These include jamming (denial), spoofing (imitating), and hijacking (altering) data, with unencrypted data particularly vulnerable to these latter two methods. Encryption can provide security from interception and spoofing (imitation) for all types of communication, and being able to change frequencies (frequency hopping) can offer protection from some jamming techniques to ensure availability.

Syntactic Layer

The Syntactic layer contains the software protocols that enable data to be formatted to harness the properties of the Physical layer to facilitate communication between and within the Infrastructure layer. There are numerous protocols employed in computer communication with the role of each one illustrated in the Open Systems Interconnection (OSI) model. This is a theoretical model created by the International Organisation for Standardisation that describes the functions of a networking or digital telecommunications system. The model describes how data are formatted to facilitate its creation, storage, processing, transmission, display, and destruction. Each aspect has its own security implications and so provides a useful method of understanding the requirements of an end-to-end communications channel. Listed from top to bottom, the seven layers are shown in **Table 1** that together comprise aspects of the Syntactic layer of cyberspace (Finjan Cybersecurity, 2016).

Examination of the Syntactic layer's composition may reveal the use of older and perhaps less secure protocols, the currency of software components, and the efficiency of network routing algorithms. The software in use can also be an important factor as unsupported operating systems or applications can introduce well-known vulnerabilities that will not be patched. These may be susceptible to exploitation and may be used as an attack vector. As well as ensuring that the latest software state is installed, the amount and type of encryption employed will also affect security. This is because some algorithms previously considered secure have subsequently been found to contain vulnerabilities (Luenendonk, 2018). Similarly, the proportion of computers protected by antivirus software and the number of infected machines within a network should be known. Together, these will provide an indication of the state of a network's security and where improvements are needed.

Semantic Layer

So far, the layers of cyberspace that have been discussed are related to computer-to-computer communication. The Semantic layer forms the translation medium between the digital data used by computer and networking technology and the human users who consume it. It is therefore an important component in any computer system that relies on a human operator to enable data to be correctly interpreted and acted upon. The Semantic layer typically comprises computer applications and their user interfaces. As well as security, there are several other factors that go into their design including linguistic, cultural, and human factors considerations. These are all related to how a user seeks to engage with others in cyberspace to achieve their desired end state. It will involve understanding methods by which operators with different backgrounds can use similar software configured to their own unique needs.

The design of the Semantic layer not only provides an output that is useful and understandable to human operators but also acknowledges the specific circumstances of the end-user.

TABLE 1 | Comparison of data transmission technologies.

ISO layer	Role	Security example
Layer 7—Application	The component closest to the end user, such as a web browser game or productivity tool	Access controlled login control, encryption of user data and secure application development practices
Layer 6—Presentation	Prepares data from Application layer for transmission	Application independent encryption for secure transmission with access controls
Layer 5—Session	Establishes communication between two devices	Strong authentication using encrypted passwords
Layer 4—Transport	Coordination of data transfer between devices	Preventing interference of protocols that segment the data into packets by limiting access and firewalls
Layer 3—Network	Determines the route that the data will take between devices	Preventing the routing of traffic from being maliciously disrupted with filters and firewalls
Layer 2—Data Link	Provides node to node data exchange	Ensuring correct identification of nodes and filtering known malicious end points
Layer 1—Physical	The electrical and hardware specifications of the system	Physical security of components

Interactions that were previously purely mechanical now provide inputs and outputs to software control systems, and this communication also forms part of the Semantic layer. An example of this is in the automobile industry in which the amount by which the accelerator is depressed acts as a digital input to the electronic engine management system. It is this that controls the speed of the car, rather than a direct linkage between accelerator and engine. The output from the Semantic layer in this case is twofold, the cognitive appreciation of a difference in speed by the driver and a visual display from the dashboard. This speed indicator may be supplemented by an audible alarm if the car is equipped with a speed limit warning system. Similarly, voice-operated systems are now becoming more common. Here, the Semantic layer incorporates a microphone, speaker, and associated software that can translate audio commands into physical responses such as turning on lights or other electrical devices.

Being software-based, the Semantic layer is subject to similar attack vectors as for the Syntactic layer. The more complex the application is, the more vulnerabilities may exist that are at risk from exploitation by an attacker. As this layer is designed specifically for human interaction, it is also one of the easiest to be accessed by those seeking to identify weaknesses that can be harnessed. As some types of software become increasingly popular and attract worldwide use, they also become more attractive to those with malicious intent. This is because any weaknesses found will have more widespread utility and so will be able to affect a greater number of potential victims. Attacking the Semantic layer may aim to achieve several objectives. These include attempts to deny user access to data, manipulate it to display erroneous information or influence user behaviour, or exfiltrate it without authorisation for a range of motivations. These incentives include political, embarrassment, revenge, financial gain, or just for personal satisfaction and entertainment.

Human Layer

Above the Semantic component, a Human layer is added next. This demonstrates the fundamental role that the user plays in understanding the nature of cyberspace and its security. As an artificial environment, cyberspace is dependent upon people and requires their intervention for all aspects of its existence and destruction. The Human layer also forms the conduit to the other physical environments. Experiences here will affect how operators interact with cyberspace and how they interpret the data that they are presented with. Understanding the attributes of the Human layer also affects how the Semantic layer is designed. It can be easier to alter a software interface once to be more intuitive and better understood by all users rather than retrain each one to understand complex, specialist applications. This layer also presents a major security threat to an entire system as it potentially contains the greatest range of vulnerabilities. Human operators are open to a variety of influences that cannot be totally predicted or prevented. Such threats include social engineering, curiosity, bribery, and blackmail as well as the normal Human traits of error and negligence. Although the inclusion of security features in software design can to some extent mitigate these issues at the Semantic and Syntactic layers, it will not provide total protection. For a comprehensive approach, some of the most effective measures to prevent a successful attack are through education and supervision at the Human layer. This emphasises the importance of training users at all levels to be able to engage effectively and safely with cyberspace. A programme of instruction designed to provide an appreciation of the capabilities and limitations of the cyber environment is essential and can affect how attitudes to the technology are formed. For the generation at school today, the so-called "digital natives," their familiarity with the use of smart phones and social medial applications is significant. These devices and the software they contain demonstrate the skill of those designing the Semantic layer to be intuitive and requiring no formal instruction to be effectively used. However, familiarity breeds contempt, and these same users may not understand the importance of the security settings of these same applications. The role of encryption, for example, which is essential to ensure the confidentiality of data, may not be an issue with which the casual user is familiar.

The addition of a Human layer, although it usually refers to an operator's interaction with the environment, also predicts a greater integration between technology and people in the future. User interfaces with cyberspace have moved from static hard-wired computers to mobile smart phones connected wirelessly through cellular networks or *via* Wi-Fi directly to Internet routers. 2015 saw the introduction of the Apple

Watch and heralded a new generation of practical wearable connected devices (Haslam, 2017). These have evolved from being just a novelty item used by first adopters to becoming more practical and useful devices. The next logical stage in this development has already been mooted as being implants in which users have devices inserted into their bodies and interact directly with them. Examples of this have already achieved significant publicity due to the research of Professor Kevin Warwick. In 1998, he was implanted with several devices enabling him to control external machines (Macaulay, 2017). More recently, medical advances had led to the introduction of remote patient monitoring in which measurements are taken and transmitted *via* wireless transmitters. This "telemedicine" enables pacemakers to be adjusted without invasive surgery as well as providing real-time data on patients' health (Elgharably et al., 2008, 1–4). With this and other active areas of research ongoing, the border between humans and cyberspace is likely to become increasingly blurred.

As well as the purely technical association between humans and cyberspace, there is also a cognitive connection that affects decision-making. To fully appreciate the Human layer of cyberspace, it is therefore necessary to understand the nature of relationships and how humans react and interact with each other. This involves an appreciation of behavioural science and the formation of societies with the role of sociology and psychology being particularly significant. These disciplines are well understood by software developers seeking to identify new market opportunities and working to design applications that fulfil them. Humans can be regarded as existing in cyberspace in three forms: as individuals, their persona, and the social groups they mix in with each having their own security implications.

The Individual in Cyberspace

Humans as users of cyberspace are individuals, that is, they can exist only as a single instantiation—we all have one unique identity. This single character is used for roles that may involve personal banking, e-mail, and social media accounts and may form the basis for digital signatures. The security of these credentials is therefore paramount to prevent online identity theft that can have devastating consequences for financial, personal, and business relationships. Obtaining this unique information is the aim of both criminals and state intelligence organisations, who may use many of the same techniques to acquire it. Recognising the importance and knowing how to secure personal information are of prime importance in any security programme. This can be challenging as the very nature of social media applications is to share personal information online. On their own, each piece of data may seem to be unimportant, but when combined may build up a complete profile of an individual and their personal preferences. Users can be particularly vulnerable to a range of social engineering attacks that target personal information or credentials to enable attackers to exploit these details to their advantage. This type of attack can be mitigated through a combination of social and technical measures. Regular awareness training can reduce the risk of comprise, and when combined with measures such as multiple-factor authentication is regarded as the most effective way to ensure personal security.

The Persona in Cyberspace

As well as having unique individual characteristics, a single person can have multiple personas. A persona is a role or a function that may be shared with many other individuals. Examples of a persona include professional activities such as lawyer, teacher, or student. Family and leisure activities can also be included such as father, mother, and dog owner. Personas are important in forming the basis for wider interpersonal relationships. They also form a key role in crafting more personalised social engineering attacks. An individual may not respond to a generic e-mail designed to harvest sensitive information, but they may be more susceptible to one that refers to a personal interest.

The Social Group in Cyberspace

Finally, it is the social characteristic, which describes how people mix in groups based on their personas. Whereas each person is an individual and each one may have multiple personas, groups are where they combine. Universities, family groups, gym memberships, sports supporters' clubs are all examples of social groups. Combining the characteristics of people, persona, and social elements can be very powerful in determining future behaviour. This was brought starkly to light in 2018 in the so-called "Cambridge Analytica scandal." After acquiring the Facebook data of millions of Americans without their permission, the company allegedly used this information about individuals, their persona, and social groups to predict their personalities. This was then used to produce highly targeted advertising intended to influence their behaviour including voting intentions (Kaiser, 2019, 26). The realisation of how the Human layer of cyberspace could be manipulated resulted in US Congressional hearings and a period of reflection on the power of the medium.

Mission Layer

The final layer of this model of cyberspace is an overarching feature that governs the relationship that we have with it and is termed Mission. This again demonstrates the artificial nature of cyberspace and that the medium was designed and constructed to fulfil a purpose. Every interaction that a human user or automated devices have with the connected environment is to fulfil a role, and there is a purpose behind every event. By understanding the reasons why a person or device engages with cyberspace, the other layers are contextualised, and the overall security requirements can be understood and formulated. The Mission layer is therefore not part of cyberspace but is essential in explaining the attributes of the other seven layers in terms of understanding its use. Although all the layers have a role to play in enabling cyberspace to function, there is a variation of dependence between them. For example, the form of the Infrastructure layer is reliant upon the Geographic

TABLE 2 | Adding a notion of distance to cyberspace.

Environment	Description
Near space	At a national level these are networks and systems that are considered vital to support critical national infrastructure and services. They are assumed to be controlled and protected by governmental agencies. At a local level, this is the element of the network that is owned and configured by individual corporations and users. These organisations and individuals exercise control the type of software and devices that are installed and used. At a personal level, this comprises individual personal electronic devices connected to the Internet
Mid space	These are defined as networks and systems critical to access global cyberspace but over which there is no local or personal control or protection. Typically, these may be geographically distant and owned by a foreign commercial company or a third-party state
Far space	The networks and systems that are the destination for communication or where an adversary may be located and is regarded as their Near space. In military operations, this is the target area that must be influenced or controlled, either temporarily or permanently

layer, but the Syntactic layer has no regard for the type of terrain in which it is formatting, encrypting, and routing data. Some data may also flow between the Infrastructure and Services layer to control the facilities that enable the networks to function but serves no wider purpose and has no human interaction. However, every part of cyberspace is reliant on the properties of the Syntactic and Physical layers that govern the form and format of the data within the environment.

THE SECOND DIMENSION—DISTANCE IN CYBERSPACE

The properties of the seven layers of cyberspace, plus the Mission layer described so far, can be applied to any location, but the same characteristics may not apply elsewhere. In the era of instantaneous communications, distance is often disregarded and the path that data follows from source to destination may not be considered. However, these attributes are important and may affect access, which may be limited by a range of factors. These include the types of fixed infrastructure, and in wireless communications, regional variations in bandwidth, coverage, and power limitations. Filtering and censorship may also vary at different points in a transmission path affecting access to an audience. This is considered in the second dimension of this model of cyberspace that adds a representation of distance. The key advantage of including the notion of physical separation between users is that it enables the properties of the layers to be considered separately at different locations. The terms used are described in **Table 2** and introduce the concept of Near, Mid, and Far geographic operating space. These are based on those first described in the UK Ministry of Defence's Cyber Primer (Development, Concepts and Doctrine Centre, 2013, 7).

As Near space defines the networks under personal or local control, this is the area in which cyber security efforts are concentrated. To achieve this, it is vital that there is a comprehensive understanding of the properties of the seven layers of cyberspace, the users active in it, and their mission. This could be as simple as in a home environment knowing who has access to each device or who is connected to a domestic router or Wi-Fi network. Corporations need to know who is on their network, with what type of computer, and how they are using them. From a national perspective, control of Near space is vital to protect the security of national or local interests from attackers and those who would wish to illicitly infiltrate it. In all cases, security is dependent upon securing every part of Near space as well as the borders with Mid space.

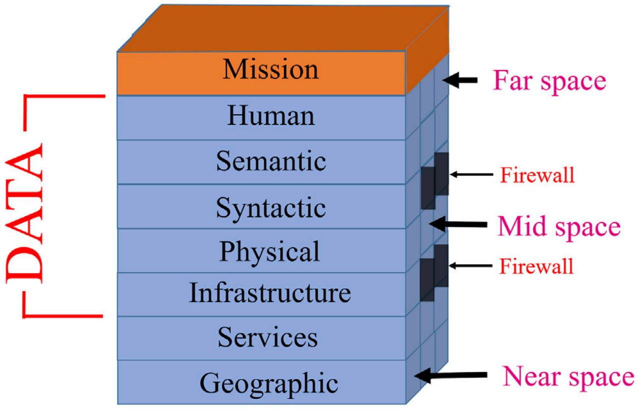

FIGURE 2 | The concept of distance in cyberspace.

Definitions of Near, Mid, and Far space depend on where control ends and may be a matter of perspective. Near space is the originator of a communication, and Far space is the destination. However, for the receiver of a message, their own network is Near space for them. Far space is also from where an attack originates with the malicious actor launching their campaign from what they would regard as their own their Near space. For both law-abiding users, state organisations, and criminals, there is a problem how to determine the properties of Far space. For legitimate users, cyberspace has evolved with compatibility a foremost consideration. Each level of the model has evolved to facilitate seamless communication using compatible applications at the Semantic layer and common protocols at the Syntactic Layer. The properties of the Physical layer are universal, and standard connections enable the

Infrastructure layer to support data exchange. Interfaces have been designed to enable backwards compatibility between legacy technology enabling Near and Far Space to interconnect. The same is true for Mid space. This is the part of cyberspace that is under the control of a third party and forms part of the Infrastructure layer that must be crossed to reach the destination. Of course, for that third-party individual or organisation, this is their Near space. For malicious parties trying to determine the properties of the Near space of their target, various tools and techniques have been developed to scan and penetrate their networks. This can be achieved remotely or through local access, but success depends on understanding the properties of the seven layers with the Mission being unauthorised access.

When considering the attributes of Near, Mid, and Far space from a security perspective, the unique risk presented by insider threats becomes apparent. Although by definition, an attacker will launch their attack from their Near space into the Near space of their victim, the properties of both may be the same. Thus, there may be no firewalls or other security control between attacker and target. In addition to implementing personnel security procedures, this also emphasises the importance of technical measures. This may involve identifying high-value components of the infrastructure such as data storage areas and segmenting or introducing other security measures to this aspect of the network. The properties of Near space are therefore reduced to a minimum and reduce the ability of an insider to access information without being documented or requiring additional access authority.

By combining the seven vertical layers and the Mission layer with the three horizontal components of cyberspace, the environment can be illustrated in two dimensions as shown in **Figure 2**. It is important to note that this model may not necessarily be regarded as a map through which a path through cyberspace can be traced. Instead, each element of the environment should be considered as a separate, discrete entity that needs to be protected individually. **Figure 2** also shows the layers that contain data and which ones may be protected by a Firewall. A firewall is a system or combination of systems that enforce a boundary between two or more networks. Typically, it forms a barrier between a secure and an open environment such as the Internet (ISACA, 2021). When used, this is one way in which the separation between Near, Mid, and Far space can be defined. A Firewall works by examining data that pass through it and by applying a set of rules tries to identify it as benign or malicious. Firewalls can be either hardware- or software-based and are only effective at the Syntactic and Infrastructure layers of cyberspace. However, data are found in every layer from Human to Infrastructure, which emphasises the need for additional security measures. Encryption can protect the Physical layer from interception, and patching software to the latest security state will secure the Semantic layer. It is at the Human layer that technology can fail if poor user understanding or behaviour results in a compromise. Protection here is reliant upon the knowledge of the threat combined with training to develop a culture of security awareness.

THE THIRD DIMENSION—UNDERSTANDING THE THREAT

The model of cyberspace that has been developed so far has enabled the properties of the environment to be examined as data pass from source to destination. However, throughout this journey, there may be numerous threats that must be considered and risks to security that must be mitigated. As the use of cyberspace has expanded into every aspect of modern society, multiple malicious actors with a range of motivations and skillsets may be encountered that must be considered. Much has been written on the different categories of cyber attackers, and what they aim to achieve. They may be internal or external to an organisation and driven by financial gain, politics, religious ideology, reputation, revenge, nationalism, entertainment, boredom, curiosity, or just for the challenge. Their skill sets may range from just using tools readily available online to developing their own bespoke means to exploit a target's vulnerabilities. However, regardless of the catalyst for their actions, it can be argued that their objectives will fall into one of three categories.

In his seminal 2013 book, "Cyber war will not take place," Thomas Rid argues that conflict in cyberspace will always fall short of the accepted definition of warfare (Rid, 2013). Instead, he proposes that offensive acts in cyberspace will fall into one of three categories: espionage, sabotage, and subversion. Although Rid's focus was on nations engaged in offensive cyber operations, it is possible to categorise every malicious action as falling broadly into one of these three classifications. Espionage, he defines, is an attempt to penetrate an adversarial computer network or system for the purpose of extracting sensitive or protected information. Although he is referring to state-sponsored intelligence-gathering operations, this explanation could be expanded to apply to all forms of data theft. Sensitive or protected information could include at an individual level banking details to enable financial loss, personal details to facilitate identity theft, or other compromising material for blackmail. Corporations are also at risk from direct financial loss but in addition face the threat that their valuable Intellectual Property could be stolen. This could result in another organisation producing a similar product, but at a lower price, as they do not have to recoup the initial investment in research or development. Companies are also at risk if customers' personal details are stolen as they will then be in breach of data protection regulations and liable for prosecution. At the national level, states targeted by espionage could be at a strategic disadvantage if details of military capabilities or positions on trade negotiations are exposed.

With regards to sabotage, Rid's definition is very narrow as the deliberate attempt to weaken or disable an economic or military system. However, expanding this statement to include targeting the function of any of the layers of cyberspace will encompass the full range of potential threats. This could involve activities such as interrupting power supplies at the Services layer or damaging components at the Infrastructure layer to jamming radio transmissions at the Physical layer. Malicious software could be used at the Syntactic or Semantic layers, and key workers could be incapacitated at the Human layer. The effects of these attacks could be temporary or permanent, but the aim will always be to have an adverse effect on the victim to achieve a desired end state.

The final category of offensive action that Rid identifies is subversion. This he describes as the deliberate attempt to undermine the trustworthiness, integrity, and the constitution of an established authority or order. Focusing more widely on actions in cyberspace, this can be redefined as undermining the reputation or trust in a target through the creation, destruction, or manipulation of digital information. This can then include illegally accessing websites, e-mail servers, or databases to add, remove or alter information, writing malicious social media posts, or generating false images. This last category of manipulating digital images or videos, the so-called "deep fakes," is particularly concerning. Although most examples seen so far have had a limited effect or have been swiftly identified as false, they are becoming more prevalent, and their quality is improving. The author predicts that deepfakes may be used in five ways in the future. The first is to produce multiple conflicting storylines to disguise the truth or to overwhelm a media outlet. The second is a "surgical strike" to strongly promote a single narrative as part of a wider influence campaign. The third is to produce convincing media to reinforce existing biases of a target audience to the adversary's advantage. The fourth is to undermine the credibility of an individual or cause through the production of obviously fake but amusing material such as memes. Finally, they can be used as an excuse by suggesting that any incriminating, but truthful, material can be disregarded as fake, the so-called "liars dividend." In parallel with advances in the production of deepfakes, an industry has developed to detect artificial media and mitigate its impact. More concerning though is that if they become too widespread, they will undermine trust in all online content. This may then result in target groups becoming vulnerable to other forms of influence activities resulting in a change in perceptions, opinions, or behaviour to the benefit of an attacker. It is important to consider that subversion is essentially an underhand activity intended to achieve an effect through false or misleading activity. Open, fact-based discussion and debate leading to informed decision-making are not a subversive activity.

Countering the threats of espionage, sabotage, and subversion in cyberspace can be effectively achieved by personnel trained in cybersecurity, which in turn can only be successful from understanding the environment. To be able to counter the threat to networked systems, security practitioners have traditionally referred to what has been termed the "CIA triad" of information security principles. This seeks to protect the confidentiality, integrity, and availability of data with each element being identified in a series of separate articles and becoming well developed by 1998 (Fruhlinger, 2020). Drawing on ISACA's glossary of terms, confidentiality is defined as Preserving authorised restrictions on access and disclosure, including means for protecting the privacy and proprietary information (ISACA, 2021). Integrity is defined as the guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity. Finally, availability is defined by ISACA as ensuring timely and reliable access to and use of information. Maintaining availability encompasses all layers of cyberspace and emphasises the importance of understanding its composition and attributes. This applies not only at the source and destination of an information exchange but also to the path in between.

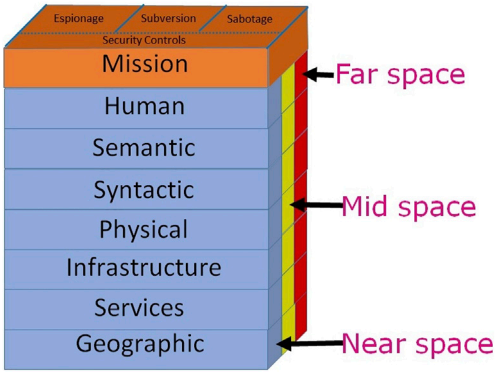

FIGURE 3 | The completed three-dimensional model of cyberspace.

Despite the CIA triad still being widely quoted, commentators were quick to identify its shortfalls and propose additional security principles that should also be considered. In 1983, Donn Parker proposed a six-sided model that was later dubbed the Parkerian Hexad, which expanded the CIA model to include possession or control, authenticity, and utility (Parker, 1983). Possession considers the idea that confidential material can be held and controlled by an unauthorised individual or party but without violating or breaching confidentiality. Authenticity involves proof of identity, and the assurance that a message, transaction, or other exchange of information is from the originator that it claims to be from (Pender-Bey, N.D). Finally, utility refers to the usefulness of the data. This highlights that information may be available and therefore usable, but it doesn't necessarily have to be in a useful form to be defined as available (Parker, 1983). The US National Institute of Standards and Technology also considered the CIA triad and added two further elements: accountability and assurance. The former is the requirement that the actions of an entity should be uniquely traceable back to them. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, after-action recovery, and legal action. Assurance is the confidence that other technical and operational security measures work as intended to protect the system and the information it processes (National Institute of Standards and Technology, 2001). More recently, the issue was again addressed, identifying seven categories of security threats comprising denial of authorised access, forgery, repudiation, spoofing, unauthorised access, unauthorised disclosure, and unauthorised modification. The author identified that the CIA triad does not defend from the security threats of spoofing, forgery, repudiation, and unauthorised access. These are overcome by the inclusion of authenticity and access control, which aligns with Parker's definition of possession (@RealWorldCyberSecurity, 2020).

The threat posed by espionage, subversion, and sabotage, and the counter activities of the security controls described above form the third dimension of cyberspace. **Figure 3** illustrates the completed model of the environment. Together, they demonstrate the complexity of cyberspace and the threats that must be countered to protect the information within it. As each malicious actor will be unique in their motivation, exploits used, timing, and objective, so the mitigation measures will also need to be individually tailored to counter them. To fully allay each one, the three dimensions of the model must be fully understood, and a key element of this is the use of threat intelligence. Threat intelligence can be defined as evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice about an existing or emerging menace or hazard to assets (Gartner Research, 2013). This intelligence informs decisions regarding the subject's response to that particular threat and enables cybersecurity assets to be most efficiently deployed. Such are the range of potential threats that a risk-based approach is needed to identify particularly vulnerable assets or those areas most likely to be used as an attack vector. Based on this information, data are collected from a variety of internal and external sources. These may include network logs, past incident reports, and research on both the open and the so-called "dark" web. These raw data are then processed using both automated and manual resources before further analysis to search for potential security issues. Finally, the completed product is disseminated, and feedback collated (Recorded Future, 2021). To be most useful, threat intelligence should be tailored to a particular audience and can be Strategic, Operational, or Tactical in nature. In UK parlance, Strategic is broad and intended for a nontechnical audience, Operational details the tactics, techniques, and procedures of threat actors, and Tactical contains details about specific attacks and campaigns. For the US audience, the definitions for Operational and Tactical are reversed.

The effective use of threat intelligence will inform an organisation of the security controls that need to be applied to counter the perceived threat to their own Near space. The model proposed in this chapter can both inform the types of information that should collected and processed as well as how the intelligence itself translates into effective security controls. Each component of the model can be used as a basis to inform decisions on where to collect threat information as well as identify areas that are weak or most susceptible to attack.

Based on the output of threat intelligence, each organisation should seek to develop their own defence methodology focusing resources where needed. This will be tailored to their unique circumstances and will require an appreciation of the threat from each layer of the model in Near, Mid, and Far space. This would then be assessed in terms of the risk from espionage, sabotage, and subversion with each one leading to a series of mitigation measures. Once that stage is complete, a security training programme can be developed to ensure that all personnel in the organisation are fully equipped to counter the actions of malicious actors.

DISCUSSION

Since its original inception as a means to connect remote computers, what is now known as cyberspace has developed beyond its creators' initial design. This growth has been haphazard and has developed according to user needs, technological advances, and the imagination of visionaries who could see its greater potential. Without a grand design, attempts to understand, model, and explain cyberspace have always lagged behind the reality of its true nature. Descriptions of cyberspace have moved beyond the purely technical to include human and cultural elements governed by a multitude of national and international policies and regulations. This presents researchers, industries, and policymakers with incomplete, often contradictory information within a constantly changing, interdependent architecture of seemingly unrelated components. These act to both facilitate and restrict communication, and when trying to consider every aspect, it becomes what has been described as a "wicked" problem. Solutions to such problems have been termed as being at best better or worse, not true or false (Churchman, 1967).

This chapter has presented a novel three-dimensional model of cyberspace with a focus on defending information from both internal and external threats. The seven core layers, Geographic, Infrastructure, Services, Physical, Syntactic, Semantic, and Human, are contextualised by a Mission element to describe every component of the medium. This allows each aspect to be examined both individually and in relation to the others as not every layer may be relevant in every situation. For example, an automated industrial control system may not require human intervention in normal operation. However, maintenance and updates will be required at some point, and this will introduce additional risks that must be considered. To fully appreciate cyberspace at any specific time and location, the attributes of each layer should be understood and how they are likely to change. This combined understanding can be referred to a "cyber situational awareness."

The second dimension of the model demonstrates that cyberspace does not exhibit universal characteristics, but that its structure and use may differ at the source and destination of an information exchange. The notion of distance using the concepts of Near, Mid, and Far space emphasises that not all components of cyberspace are under the control of the originator of a message. This understanding of the properties of cyberspace at different geographical locations enables the security threats and risks for each to be separately analysed. It also highlights that the environment at the destination in terms of bandwidth, language, equipment, and availability of service may differ from that at the origin of a communications channel.

The third dimension of the cyberspace model focuses on the security aspect by examining the threats and their countermeasures at each layer and location. By linking espionage, subversion, and sabotage with a range of security controls, it links each threat with one or more mitigating actions. Using this third dimension within the context of the other two, it enables a comprehensive risk assessment to be made and then countered according to an assessment of the threat. The three dimensions highlight its pluralistic nature with many groups of individuals, organisations, and governments competing for access and control. It has caused multiple paradigms shifts in both academia and industries. Although the layers may appear distinct and separate, there may be blurred lines between them, and in a real world, they are constantly changing. Thus, any measurement is only a snapshot in time and can only approximate its true nature. This presents a challenge when considering its security aspects, which may also vary with time. Cybersecurity comprises a balance between seemingly contradictory requirements. There may be a desire to be transparent, but also implement security in some areas, privacy competes with open access, and should cyberspace be a public space or private property. To address these complex problems, this model provides an abstraction of the properties of cyberspace and enables the factors that must be considered to be visualised and understood. By assessing each layer in terms of Near, Mid, and Far space within the context of the threat provides an understanding of what cybersecurity measures are needed. This in turn will influence, either directly or indirectly, the training requirements of those using the medium to fulfil their mission. These can range from specialist technicians able to configure complex systems to the standard user of the network. This model can assist in determining the training requirements of all those working within an organisation as well as those tasked with protecting the communications channel. Utilising the information that the model can provide, it can ensure that the training offered is relevant and appropriate for the purpose.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, and further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

@RealWorldCyberSecurity (2020). What Are the Fundamental Services provided by Security? Hint: CIA Is Not the Answer. Mar 25. Available at: https://medium.com/@RealWorldCyberSecurity/what-are-the-fundamental-services-provided-by-security-hint-cia-is-not-the-answer-413d1a0355d (Accessed Sep 18, 2021).

Balandin, A. A. (2009). Chill Out. *IEEE Spectr.* 46, 34–39. doi:10.1109/mspec.2009.5267996

Bigelow, B. (2018). “The Topography of Cyberspace and its Consequences for Operations,” in 10th International Conference on Cyber Conflict. Editors T. Minárik, L. Lindström, and R. Jakschis (Tallinn: CCDCOE), 123–138. doi:10.23919/cycon.2018.8405014

Blum, A. (2012). *Tubes*. London: Penguin.

Brady, W., and Elkner, J. (2017). History of the Internet. Available at: http://openbookproject.net/courses/intro2ict/internet/history.html (Accessed June 12, 2020).

Cabinet office of Japan (2021). Society 5.0. Available at: https://www8.cao.go.jp/cstp/english/society5_0/index.html (Accessed Sep 18, 2021).

Churchman, C. W. (1967). Guest Editorial: Wicked Problems. *Manage. Sci.* 14 (4), B141–B142. http://www.jstor.org/stable/2628678.

Development, Concepts and Doctrine Centre (2013). *Cyber Primer*. Shrivenham: Ministry of Defence.

Elgharably, R., Marzban, E., Belal, S., Ahmad, B., AbdElLatif, I., Atef, R., and ElBabli, I. (2008). “Wireless-Enabled Telemedicine System for Remote Monitoring,” in Cairo International Biomedical Engineering Conference (Cairo: IEEE), 1–4. doi:10.1109/cibec.2008.4786070

FBI (2014). Update on Sony Investigation. Available at: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation (Accessed June 12, 2020).

Finjan Cybersecurity (2016). Application Layer Security and the OSI Model. October 11. Available at: https://blog.finjan.com/application-layer-security-and-the-osi-model/ (Accessed August 30, 2021).

Fruhlinger, J. (2020). The CIA Triad: Definition, Components and Examples. Feb 10. Available at: https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html (Accessed 09 18, 2021).

Gartner Research (2013). Definition: Threat Intelligence. May 16. Available at: https://www.gartner.com/en/documents/2487216/definition-threat-intelligence (Accessed Sep 18, 2021).

Gates, B. (1976). An Open Letter to Hobbyists. January. Available at: https://genius.com/Bill-gates-an-open-letter-to-hobbyists-annotated (Accessed June 12, 2020).

Gibson, W. (1994). *Neuromancer*. London: Harper Collins.

Global Security (2011). CBU-94 "Blackout Bomb" BLU-114/B "Soft-Bomb. Available at: https://www.globalsecurity.org/military/systems/munitions/blu-114.htm (Accessed June 14, 2020).

Google (2021). Your Internet. For Everything. Available at: https://fiber.google.com/ (Accessed August 30, 2021).

Greenberg, A. (2019). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin’s Most Dangerous Hackers*. New York: Doubleday.

Haslam, K. (2017). Original Apple Watch Review. July 31. Available at: https://www.macworld.co.uk/review/apple-watch/original-apple-watch-review-3544044/ (Accessed June 14, 2020).

ICRC (2021). Practice Relating to Rule 1. The Principle of Distinction between Civilians and Combatants. Available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule1_sectiona (Accessed August 30, 2021).

ISACA (2021). Glossary. Available at: https://www.isaca.org/resources/glossary#glossf (Accessed August 30, 2021).

IT Pro (2017). TalkTalk Hack: Two Men Plead Guilty to TalkTalk Hack. April 27. Available at: https://www.itpro.co.uk/security/24136/talktalk-hack-two-men-plead-guilty-to-talktalk-hack (Accessed June 12, 2020).

Kaiser, B. (2019). *Targeted*. New York, NY: Harper Collins.

Katzman, S. (2016). *Operational Assessment of IT*. Boca Raton, Fl: CRC Press.

Kramer, F. D. (2009). “Cyberpower and National Security: Policy Recommendations for a Srategic Framework,” in Cyberpower and National Security. Editors F. D. Kramer, S. H. Starr, and L. Wentz (Dulles, Washington: Potomac), 4.

Lawfare (2021). Lawfare. August 30. Available at: https://www.lawfareblog.com/ (Accessed August 30, 2021).

Leiner, B. M., Cerf, V. G., and Clark, D. D. (1997). Brief History of the Internet. *Internet Soc.*. Available at: https://www.internetsociety.org/internet/history-internet/brief-history-internet/ (Accessed June 12, 2020).

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Luenendonk, M. (2018). 5 Common Encryption Algorithms and the Unbreakables of the Future. December 20. Available at: https://www.cleverism.com/5-common-encryption-algorithms-and-the-unbreakables-of-the-future/ (Accessed June 14, 2020).

Macaulay, T. (2017). Meet Captain Cyborg: the Man that Biohacked His Own Body. May 24. Available at: https://www.computerworld.com/article/3557996/meet-captain-cyborg-the-man-that-biohacked-his-own-body.html (Accessed June 14, 2020).

National Institute of Standards and Technology (2001). *Underlying Technical Models for Information Technology Security*. *Special Publication 800-33*. Washington, DC: US Department of Commerce.

NATO HQ (2021). Cyber Defence. July 02. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm (Accessed September 31, 2021).

NATO Standardization Office (2020). *AAP-06, NATO Glossary of Terms and Definitions*. Brussels: NATO Standardization Office (Accessed August 30, 2020).

Offensive Security (2021). Kali Linux. Available at: https://www.kali.org/ (Accessed August 30, 2021).

OpenNet Initiative (2014). Research and Data. Available at: https://opennet.net/ (Accessed June 20, 2020).

Oxford English Dictionary (2021). Oxford English Dictionary (Online). Available at: https://www.oed.com/ (Accessed 08 30, 2021).

Parker, D. B. (1983). *Fighting Computer Crime*. New York: Scribner.

Pender-Bey, G. (). The Parkerian Hexad. Available at: http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf (Accessed Sep 18, 2021).

Peters, S. (2014). Sony Hackers Knew Details of Sony's Entire IT Infrastructure. April 12. Available at: https://www.darkreading.com/sony-hackers-knew-details-of-sonys-entire-it-infrastructure-/d/d-id/1317898 (Accessed June 12, 2020).

Recorded Future (2021). What Is Threat Intelligence? Available at: https://www.recordedfuture.com/threat-intelligence/ (Accessed Sep 18, 2021).

Rid, T. (2013). *Cyberwar Will Not Take Place*. London: Hurst.

Schmitt, M. (2013). "Tallinn Manual on the International Law Applicable to Cyber Warfare," in *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press). doi:10.1017/CBO9781139169288

Sheldon, J. B. (2011). Deciphering Cyberpower. *Strateg. Stud. Q.* 95.

Singh, M. (2021). www.techcrunch.com. January 2. Available at: https://techcrunch.com/2021/01/21/google-alphabet-is-shutting-down-loon-internet/ (Accessed August 30, 2021).

Society 5.0 (2021). Society 5.0. Available at: https://www.conference-society5.org/ (Accessed Sep 18, 2021).

Stang, G. (2013). Global Commons: Between Cooperation and Competition. April. Available at: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_17.pdf (Accessed April 12, 2020).

Starks, T. (2018). U.S. Indicts North Korean National for Sony Hack, Massive Cyberattacks. June 9. Available at: https://www.politico.com/story/2018/09/06/justice-department-north-korea-sony-hack-771212 (Accessed June 12, 2020).

Strassmann, P. A. (2009). The Internet's Vulnerabilities Are Built into its Infrastructure. November. Available at: https://www.afcea.org/content/internets-vulnerabilities-are-built-its-infrastructure (Accessed June 14, 2020).

Townsend, C. (n.d.). A Brief and Incomplete History of Cybersecurity. Available at: https://www.uscybersecurity.net/history/ (Accessed June 18, 2020).

Travel China Cheaper (2021). List of Websites and Apps Blocked in China for 2021. August 1. Available at: https://www.travelchinacheaper.com/index-blocked-websites-in-china (Accessed August 30, 2021).

UN System Task Team (2013). Global Governance and Governance of the Global Commons in the Global Partnership for Development beyond 2015. Available at: https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf (Accessed June 12, 2020).

US Department of Justice (2018). North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions. September 6. Available at: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (Accessed June 12, 2020).

US-CERT (2020). Guidance on the North Korean Cyber Threat. June 16. Available at: https://www.us-cert.gov/ncas/alerts/aa20-106a (Accessed June 18, 2020).

Withers, P. (2015). What Is the Utility of the Fifth Domain? *Air Power Rev.* 18 (1), 126–150. Available at: https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/documents1/air-power-review-vol-18-no-1/ (Accessed June 14, 2020).

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.