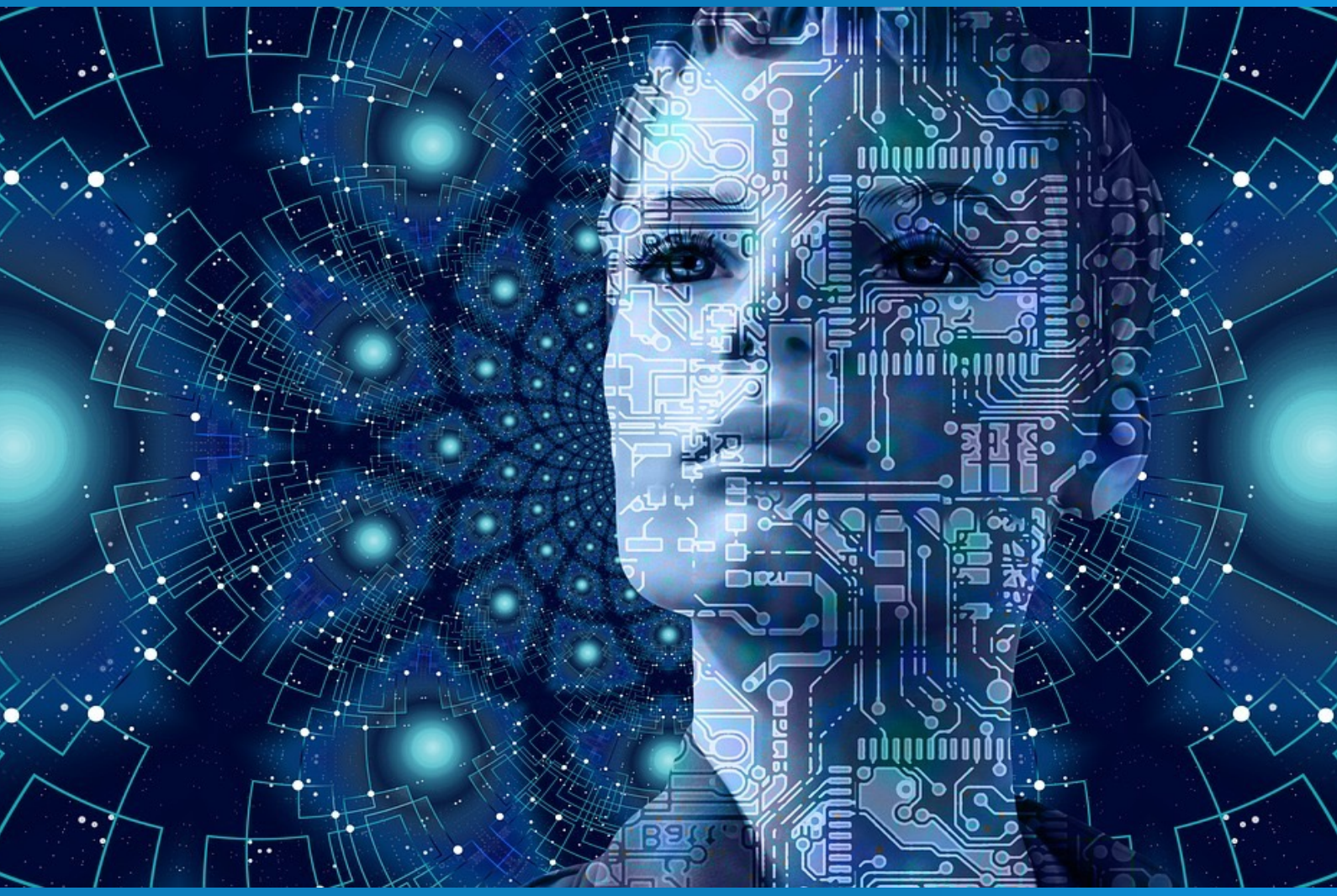
WHITE PAPER

The Fourth Industrial Revolution & Cyberspace's Mental Health Stigma



Christina Boguszewicz | Marek Boguszewicz | Zaheema Iqbal

Sarmad Khan | Rafia Nauman

Image Source: unsplash.com

Global Foundation For Cyber Studies And Research®

About the Authors

Dr Christina Liang-Boguszewicz, is the Partner and Group Managing Director of BI Group, is a seasoned Business Transformation leader, a trusted C-level Gatekeeper/Adviser, and a Business Psychologist with over 15+ years of leadership experience. She has a good track record of successfully turnaround activities. She is known for her UAIME technique and is one of the pioneers in Asia to combine Science and Technology in transforming organization into a Profitable, Resilient, and SMART Corporation. She champions in aligning Organization Growth with Human Capital x IoT x Blockchain and has delivered projects globally. Her notable clients range from luxury, financial, technology, real estate, consumer, FMCG, wellness, and retail. Dr Christina is the Chief Corporate Affairs Officer, Chair of Cyber Psychology & Cyber Space Mental Wellness (CyPSYCH) Special Interest Group and Policy Expert at the Global Foundation of Cyber Studies and Research Washington DC. She is also author of the book 'Fostering the Wisdom of Resilience'

Marek Boguszewicz, is one of the world's top experts in digital transformation and cyber security, a senior technology executive / adviser / speaker with over 30 years of experience in Technology-Finance, Digital Transformation, Cyber Security, Blockchain and NextGen 3.0 DLT Technology. Marek is the Senior Partner / Chief Cyber Security Officer / Digital Officer of BI Consulting Group, a global Strategy and Consulting firm located in Singapore with a global footprint. He works closely with leaders and board of blue-chip companies, financial services, insurance, government agencies and who's who from wall street. Marek is the Co-Chair of Cyber Psychology & Cyber Space Mental Wellness (CyPSYCH) Special Interest Group and a policy expert in ISMS, ISO27001, ISO90001 and Cyber Security Culture at the Global Foundation of Cyber Security Studies & Research Washington DC.

Zaheema Iqbal, is a senior cyber security policy researcher at National Institute of Maritime Affairs, Bahria University Islamabad, Pakistan. She is the graduate of National Defense University, Islamabad. *She regularly writes for national and international platforms, academic journals and* is one of the authors of a book "Sustainable Development in a Digital Society" in which she contributed a chapter "Cyber Threats to Pakistan's Digital Landscape". *Her areas of interest include* cyber governance, cyber terrorism, data governance, and emerging technologies. Zaheema, is the Head of Marketing and Communication, Co-Chair of Cyber Psychology & Cyber Space Mental Wellness (CyPSYCH) Special Interest Group and senior policy researcher at Global Foundation for Cyber Studies and Research Washington DC.

Sarmad Ali Khan, is an independent researcher working on international security with a focus on transformation of security landscape in Asia-Pacific. Previously, he worked at the South Asian Strategic Stability Institute (SASSI) University as a Research Fellow. The primary area of his work includes: (i) Cyberspace Strategic Competition between U.S and China; (ii) Transforming Deterrence Stability in South Asia; and (iii) Emergence of New Security Alliances in Asia Pacific. He also works on Non-Kinetic Warfare with a focus on the role of Cyber & Disruptive Technologies in Military Affairs. He has multiple international research publications to his credit. He is pursuing his M.Phil. Degree from Bahria University, Islamabad Campus. Sarmad is currently conducting research on topics such as the fusion of cyber, electronic and disruptive technologies in warfare and their impact on military doctrines and operations. He is also a policy researcher at the Global Foundation of Cyber Studies and Research. He can be reached on Email.

Rafia Nauman, is a psychologist by profession having expertise in various fields. She has more than a decade's experience of content writing. And has worked for various organizations including work related to cyber space and mental health. She has been a part of the translation team for COVID studies with the Psychological Science Accelerator. As an early year's faculty member, she has worked as an assistant teacher for kindergarten at Beaconhouse School System along with being an English Language Facilitator. Her areas of expertise include mental health arising disruptive technologies and business psychology. Rafia, is a policy researcher at the Global Foundation of Cyber Studies and Research. Her areas of expertise include mental health arising disruptive technologies and business psychology.

About GFCyber

Global Foundation for Cyber Studies and Research is an independent, non-profit and non-partisan policy research think tank for Cybersecurity studies, located in the Washington D.C, USA.

Cover Design & Styling: Amanullah Quadri

Citation Style:

Boguszewicz C., Boguszewicz M., Iqbal Z., Khan S., Nauman R., "The Fourth Industrial Revolution & Cyberspace's Mental Health Stigma", Global Foundation for Cyber Studies and Research, April 2021.

Table of Contents

Abstract

The Fourth Industrial Revolution (Industry 4.0) is the progressive automation of traditional manufacturing and industrial processes using modern intelligent technologies. Large-scale machine-to-machine communication (M2M) and the Internet of Things (IoT) will be integrated to increase automation, improve communication, monitor production itself, and develop intelligent machines that can analyze and diagnose problems without the need for human intervention. The phrase "Fourth Industrial Revolution" was introduced by a team of scientists who developed a high-tech strategy for the German government.

The Fourth Industrial brings a world of opportunities for organizations of all sizes to adopt technologies not only to survive, but thrive. This will fundamentally transform the global system of labor production, forcing job-seekers to develop new skills needed to adapt to automation. New technologies will make assets more durable and resilient, and data analysis will change the way they are managed. Physical products and services are enhanced by digital skills, thereby increasing their value. Consumers and businesses will be the customers at the epicenter of the economy, improving the way customers are served. Although big data is unrivalled in value and has propelled the industry 40% faster than any other emerging technology, its distributed structure presents a number of challenges. Security, data protection, access control and data storage.

As Cyber Security increasingly becomes part of the Socio Cyber fabric, the need of a 360-degree view in terms of Mental Health is now a social imperative. What does this mean in the real world, where we all live, work and play?

Part 1: Overview and Introduction

The Fourth Industrial Revolution has the power to change the world. However, this phase of the Industrial Revolution raises its own challenges in terms of cyber-security threats. The lack of effective cyber-security measures in IIoT-enabled production environments poses a serious threat to the new era of industrial production systems and processes. In an age of hyper-connected industries, everything is vulnerable. The world's cyber security experts are concerned about the impact of Industry 4.0. In other words, all networked industries are vulnerable to attackers who want to exploit resources and data. This is a crisis that will divide society and create instability around the world. Public confidence in business, government, media and technology will decline.

In 2020, there were 4.14 billion social media users in the world. Social media usage continues to grow alongside internet expansion, and if the rate continues, the extrapolation indicates there could be more than 4.2 billion social media users by the end of 2021.

Social media usage is so totally pervasive in all Geographies, to different levels. The most active of social networks are expanding on a daily basis with real time analytics and AI. On Twitter, **an average total of 500 million Tweets are reported daily**. Twitter at time of writing had approximately +370.9 million users on the platform. The vast number of social media users online is growing. As an example, on Facebook, *there were 2.73 billion active* users in February 2021.

With A.I. and analytics engines, geolocation, third party digital marketers, there is a clear and present danger on all digital fronts. Humans being biological entities are now experiencing the Emotional Digital

World Syndrome. Systems are interconnected at millisecond speed and one platform or application is linked to another, by direct or third party means.

Cyber security must be at the heart of people, property, government, and society in order to enable industry to securely initiate technological advances. Digital corruption and upheaval are not an option. If systems are hacked, they will perish as a result, not as an inconvenience in a vortex. The issue is not whether we fail to realize the full potential of such technologies, but how we come together as an international community to fight cybercrime and protect the digital infrastructure that forms the backbone of our world. The WEF Global Risk Report warns that the consequences of digital fragmentation and geopolitical tensions stand in the way of an international consensus on how to advance the Fourth Industrial Revolution. If it is to be a new world, we want to make it a world where we trust our digital systems and where we feel safe and secure.

This paper will help us to understand the relationship between cyberspace and mental health stigma in the fourth industrial revolution. This paper will further take us to investigate, analyze and present a call for action on Cyber Space Mental Health.

The Fourth Industrial Revolution

The Fourth Industrial Revolution heralds a series of social, political, cultural, and economic upheavals that are taking place in the twenty-first century. Building on the widespread availability of digital technologies resulting from the Third Industrial and Digital Revolution, it is driven by the convergence of digital, biological, data and physical innovations.

Artificial intelligence, genome editing, augmented reality, robotics, the Internet of Things, autonomous vehicles, 3D printing, nanotechnology, biotechnology, materials science, energy storage, and quantum computing promise better systems optimization, changes the way people create, exchange and distribute value.

Faster progress and higher computing power will lead to a more connected and complex world that will drive multisectoral and regional change in many ways, just as the start of the Fourth Industrial Revolution continued to spread access to electricity and bring the benefits of the Second Industrial Revolution to communities around the world.

Future technological innovation will produce supply-side miracles and long-term efficiency and productivity gains. Transport and communications costs will fall, logistics and global supply chains will become more effective, and trade costs will fall, opening up new markets and boosting economic growth
Like the Industrial Revolution before it, the Fourth Industrial Revolution will bring incredible opportunities for individuals, industry and nations. One of the great promises of the Fourth Industrial Revolution is the potential to improve the quality of life of the world's population and raise income levels.

The Cyber Psychology

Cyber psychology is an examination of the human mind and behavior and how technological society, in particular, augmented reality and social media, influence it. Mainstream academic findings concentrate on the psychology of people and communities on the Internet and cyberspace. Some subjects include online identities, online connections, personality styles in cyberspace, computer

transfers, computer and internet addiction, cyberspace regressive behavior, online gender-swapping, etc. In this area, statistical and analytical analysis is focused on Internet use, but cyber psychology often provides an examination of the psychological implications of artificial intelligence, and virtual realities. While some of these issues seem to be the subject of science fiction, they soon become scientific facts, as seen by interdisciplinary methods in biology, engineering, and mathematics (Riva et al., 1997). The area of cyber psychology remains open to further refinement, including research into existing and potential developments related to technology in the field of mental health.

The United States has passed the watershed 50% mark on Internet use, personal computer use, and mobile phone use at the turn of the millennium. Our views go beyond symbols and photos in our natural world to include graphs and images on the computer screen, with this extensive exposure to computers and their displays. The relevancy of human-computer (HCI) science in the field of cyber psychology will become more evident and important to explain the modern way of life of many people as the overshadowing between man and machine grows. With the number of internet and computer users worldwide, the impact of computer technologies on the human psyche will begin to affect our experiences and our beliefs as the SocioCyber construct becomes a fabric of society, ergo the so-called Society 5.0

Biometrics

virtual layers of security not only for verification but for wider purposes such as digital crime prevention and cyber security for online banking, e-commerce, and defense linkages (Kour et al., 2016). The rise of biometric identification and its gradual adoption across the globe in all domains of life has redefined the concept of authentication and cyber security. Biometrics is a combination of two Greek words; *'bios'* meaning life and *'metrikos'* which means measuring. It is defined as recognizing individuals through automation by analyzing their biological and behavioral features (D, 2020). Facial recognition, retina scans, iris and fingerprint mapping are few of the contemporary forms of biometrics whereas substantial work has been carried out to recognize individuals through their body posture, body odors, facial contortion and even through the placement of vein's (*What Is Biometrics Security*, 2021).

Despite various cybersecurity applications, vulnerabilities attached to biometrics remain aloft. Soft biometrics has matured as one of the challenges in which biometric data can be exploited to determine and use information in specific contexts. Soft biometrics have enabled the developers to determine the handedness of writers through sample signatures, have allowed determination of age through facial image and other similar application (Fairhurst et al., 2017) which facilitates the biometric forensics on one hand but carries a psychological aspect to it on the other hand. For example, age estimation through soft biometrics allows facial recognition software to predict how a person would look after a set number of years; the prediction precision has reported to range from 73% up till 93%. This creates a dilemma for individuals and groups in essence of their personal space being invaded by being constantly tapped and followed through biometrics. Similar to age prediction is the ability to gauge emotions, determine mental state and detect whether or not the user is stable through *keystroke dynamics*. The particular instrument of biometric modalities again influences human thoughts and how a particular person responds while using his/her keyboard, mouse and touch screen, subject to their awareness on the subject. However, for the general public, a lot of data is retrieved, interpreted and built-on through keystroke dynamics (Fairhurst et al., 2017).

Machine Learning

In the technology-led world interconnected with personal devices and large computing devices, billions of “data bytes are being synthesized, processed, shared and consumed” across civil and military domains in cyberspace. With extensive use of cloud computing, advanced algorithms and employment of machine learning techniques are being employed for safety and security of the aforementioned data from malware, intrusion of different sorts and authentication of end-users. Machine Learning (ML) denotes computational methods through which computers retrieve and acquire knowledge by learning human activities of the end-users. ML involves a set of different areas of study including computer sciences, psychology, statistics, and neuroscience (Dasgupta et al., 2020). ML algorithms are divided into different categorized depending upon the nature of their algorithm model ranging from pattern recognition, clustering of datasets based on similarity, image and pattern classification, data analysis of speech and text so on and so forth (Dasgupta et al., 2020). (Eyre et al., 2016) note that out of all domains, application of ML in mental health remains the largest in terms of learning and analyzing data inputs which are further refined to assist humans. One such example is the use of ML to compare statistical data of suicide risk through classification model; a study was conducted which showed that electronic health record (EHRs) were assessed to compared algorithm-based suicidal behavior of patients at 3 months with clinician prediction and it was found that the results of EHR were superior.

In the mental health domain, ML models have developed advanced datasets as they have access to diverse populations covering various age groups, genders, geographic locations and above all socio-economic classes through which both exclusive and all-inclusive approaches are developed to mitigate the risks (Thieme et al., 2020). In addition, the industrial internet of things (IIOT) has developed synchronization schemes (Qiu et al., 2018) “to monitor people with acute mental problems” so that healthcare experts have heads-up call to act in emergency situations. Moreover, to ease the functioning of healthcare experts, IIOT has developed network sensors attached with ML models and health care institutes (Srividya et al., 2018).

Artificial Intelligence

Artificial intelligence (AI) is based on the development of algorithms and computer programs to replace human intelligence to carry out tasks such as problem-solving, reasoning, language-understanding and analysis and general learning (Saleh, 2019). Artificial intelligence, as defined by Merriam Webster, states, “The capability of a machine to imitate intelligent human behavior” (*Artificial Intelligence | Definition of Artificial Intelligence by Merriam-Webster*, 2021). In artificial intelligence, the machines are composed in such a way that they are able to access information and use it in such a way that reasoning and self-alteration (modification) can be done. Artificial intelligence is being used around the globe to replace normal computers so that the machines are able to adapt in various contingencies.

How is AI affecting our social lives?

The incorporation and use of AI in our daily lives is said to be a two-edged sword as it has many advantages and set-backs at the same time. For example, AI-driven robots are being used to carry out hazardous tasks such as defusing bombs which reduces the risks associated to human life (Poola, 2017) whereas algorithm-led sentinels placed in conflict zones (Boulanin, 2019) poses a great threat to human life as these sentinels are normally programmed for hit-and-kill missions without distinguishing between green and red forces as well as armed or unarmed people. Similarly, as developments are being made in AI, more intelligent-machines and robots have started to take over

many jobs. Ultimately, massive down-sizing continues leading towards unemployment which in turn accounts for several mental health issues most notably depression, social anxiety etc.

AI is also assisting people in daily tasks such as GPS locators, typing-assistance with minimal errors, mathematic calculations (Poola, 2017), classification of pictures on social media (Smith & Eckroth, 2017), predicting pollution, forex trading predictions (Sabhnani et al., 2001), organization management in different sectors, etc. One of the key aspects of AI which is relevant for this study is its use for medical research; reports highlight that AI has contributed in diagnostics of health issues notably complex neurological disorders, measuring effects of medicines on patients' health (Hussain & Qamar, 2016) so on and so forth. Music industry has also welcomed the use of AI to compose new music and revamp existing one: "variations" module developed by Bruce Jacob applies genetic algorithms to compose music and afterwards analyze if it is up to the mark or not. By developing simulation games, in which developers have back-end access to the responses of end-users, AI enables the developers to analyze the intellect level, thinking patterns, response time and overall working mechanism of their brain in different scenarios (Sabhnani et al., 2001). According to a survey, 59% people opined that AI continues to influence human life, 24% were of the view that it did not play any role while 17% failed to recognize if AI had any role to play or not (Poola, 2017).

Cybercrime

Cyberattacks that are aimed "to compromise the integrity, confidentiality or availability of system" through malware, spyware, distributed denial-of-services attack (DDOS), hacking, or ransomware are known as cybercrime. Cybercrimes, in contemporary security settings, have become organized and evolved from civil to a strategic level whereby not only the public is affected but national institutions and critical state infrastructure of countries are also targeted (Bada & Nurse, 2019). For instance, a cyberattack infecting a power station through malware and consequently causing a power breakdown would have social and psychological effects on hundreds of thousands of people. Interruption in the supply of electricity would not only disrupt the daily working of people but would also induce anxiety, depression and at worst cases anger. It would also lead towards losing confidence in the cybersecurity apparatus of the state (Bada & Nurse, 2019).

Cyber-bullying is one of the most overlooked cybercrimes that has affected mental health to a very vast degree. Cyber-bullying has a diverse definition with respect to different regions and its targets vary based on demographic changes. It can be defined as "the use of information and communications technology to intimidate, harass, victimize or bully" others (Bhat et al., 2013). According to a study, 6% of the European youth (aged 9-16) were virtually bullied one way or the other whereas 3% admitted to have bullied someone (Lindert, 2017). A study conducted by Microsoft to examine youth being cyber-bullied highlighted, that out of 25 countries surveyed, three of the countries which reported the highest number of online bullying incidents included Asia countries namely China marking 70%, followed by Singapore at 58% and India having 53% of its youth that were cyberbullied. Cyberbullying or virtual harassment of females is another aspect of cybercrime that is usually not discussed. Many females face serious challenges while using the internet, especially the social media platforms (Bhat et al., 2013).

Intelligence without Ethics

The importance of intelligence in cyberspace has seen an upsurge to unprecedented levels compared to human intelligence. The conduct of state-level operations and people-to-people contacts through communication networks has led to the institutional approach of gathering intelligence directly through

government channels or by outsourcing the tasks. Contemporary governments are of the view that law enforcement agencies must have access to communication systems, data storage, and associated working mechanisms in totality (Abelson et al., 2015). Although this argument has faced criticism publically through protests and legally through data protection laws, there remains grave concern over the fact that governments continue to covertly conduct surveillance at many levels. Edward Snowden's revelation of American cyber surveillance over not only its population but of many other countries is one of the few examples to quote which shows that countries carry out intelligence without taking into consideration ethics, morals etc.

Trends in cyber surveillance and electronic intelligence have increased over the years with improvement in technology and have added new layers to and forms of intelligence. The focus on metadata, internet of things (IoT), and using commercial organizations (in the form of social media and gaming applications) has eased the cyber-operations of many countries. For example, the use of metadata for profiling – by accessing private and confidential information of an individual – in order to effectively govern and surveille on individuals and groups is one of the applications where intelligence is carried out through third parties (Bernal, 2016) by breaching their privacy. Moreover, country-specific legislations allow the government to access private data well-beyond the scope of public domain. For example, Investigatory Powers Bill gives the British government with extensive powers for "bulk interception, bulk acquisition of communication data, bulk equipment interference, bulk personal datasets (BPDs)" without a limit attached to its usage. It also gives thematic warrants to cover large geographical locations to collect large volumes of data (Bernal, 2016).

Intelligence through access of cameras on smartphones, laptops, and closed-circuit television (CCTV) has also become one of the important tools in cyberspace activities. Since 2001, the use of CCTVs at airports, train stations, public places have increased in Western countries and was gradually adopted all across the world. Although by using technologies like CCTV, many countries were able to strengthen their security apparatus and mitigate many terrorist activities (Stutzer & Zehnder, 2013) but the aspect of private-space infringement of the public raised concerns.

At a non-state level, commercial companies like Facebook, Microsoft, Google, Apple, Skype etc. give "direct access" of their respective servers to the U.S. National Security Agency (NSA) under the PRISM program. This allows the NSA to carry out profiling of people, analysis of their activities (Bernal, 2016), run their records against AI and ML software for trend analysis and so on and so forth. Through such massive access to civil applications, ethical intelligence becomes questionable. Effects of such extensive and round-the-clock surveillance on people are both active and passive. Moreover, intelligence through public platforms also infringes the human rights of people that are guaranteed under UN conventions.

Dark Web

The Dark Web is a general concept in which web users can communicate remotely without the general society, social a, web engine, DNS and URL that make up the so-called Light web, where most companies and people exist in. There are also websites that are not Tor-compliant, such as forums with password-protected secrets and credit card numbers, which can be used as part of the obscure network. There are several uses of the Dark Web: drug purchases and sales, encryption tools, hacking programs, child pornography, etc., many are nefarious in nature and some are not. The Dark Web, meanwhile, is "a part of the Deep Web that has been intentionally hidden and is inaccessible through standard Web browsers." Accessed by such browsers and networks such as TOR and I2P, this dark Web makes it possible for users to remain entirely anonymous. While in some cases, this

anonymity is used simply as a way to protect free speech or for government agencies to keep top-secret data under secure, the other side of the hidden web may truly be called a dark web where the bad actors, illicit crimes, criminal cyber gangs and dark society exist to ultimately do harm.

The anonymity of illicit activity on the dark web cloaks an enterprise of mounting concern to authorities. One site alone generated an estimated $219 million in annual revenue as of 2017, according to a new NIJ-supported report by the RAND Corporation (RAND). The report, “Identifying Law Enforcement Needs for Conducting Criminal Investigations Involving Evidence on the Dark Web,” explores better ways to investigate dark web crimes. Although the dark web still accounts for just a fraction of all illicit sales online, it appears poised for rapid growth, according to the report.

Deep Fake Technology

Artificial Intelligence (AI) now allows for the mass production of the so-called deepfakes: synthetic videos similar to actual videos. By providing a broad representative sample of the UK population with a new experimental procedure, we were able to assess the people's deepfakes assessments.

Deep fake is an artificial intelligence Masquerading as a legitimate source. It may have several variations such as photographs, audio, video fabrication, as well as several other media types, A portmanteau of deep learning and fake is the word that represents both the technology and the resultant false information. An example of usage is the use of a deep fake to get David Beckham to send a message about malaria by a UK medical organization. This message was sent in nine languages too. However, if some want to employ this technology for nefarious reasons, the basic software and capability is readily available. They may be used, for example in election propaganda, to transmit fake information from an otherwise trusted source. Initial review by non-technical cyber experts may pass the basic test, where stringent checks on the source validation have not taken place.

Deep technology works by using two competitive AI algorithms, one is known as the generator and the other is called the discriminator. Deepfake content is generated. The generator, which produces the falsified multimedia output, asks the discriminator if it is genuine or fake (Westerlund, 2019). The generator and the discriminator together form a generative opposing network (GAN). Whenever the discriminator correctly defines material as generated, the generator receives precious knowledge about how the next deep fabric can be improved.

The role political profoundness can inevitably play in public debate depends on how various players treat it. Technology firms are more likely to create AI tools that produce a human synthesis, but we expect that they will still use their AI to uphold the democratic good of authenticity by supporting the identification of deep policy defects. Social networking sites can decide whether automatic and human qualification and control types will promote or impede deepfake publishing and sharing. Deepfakes may include several attack vectors, including public sector chatbots, misleading videos from critics, and several variations of these. The various messages and constructs of this nature are devised in such a way that source determination may be extremely difficult to achieve.

Part 2: Public Health

Understanding Mental Health

Mental health is a state where individuals realize their abilities and are able to cope with daily stressors and are able to work productively to make a difference in the community. As humans, mental health is fundamental to our daily functioning, both individually and collectively.

Mental health is considered to be an integral part of our health. The World Health Organization defines health as a state of complete mental, physical, and social well-being and merely not just the absence of disease (World Health Organization).

In the fourth industrial revolution, where almost the entire world is connected through the internet, mental health plays a great role. There are a number of aspects which matter and jointly impact the general mental health of an individual. Especially, children and young adults especially have easy access to social media and the internet as an integral part of their lives, both for entertainment and for studies and research etc.

This in return has raised serious concerns for both, the parents and teachers as open access to the internet and social media can and has had many psychological effects on the mental health of children and young adults. (OECD, 2017) The association between screen time and poor health outcomes has been well-documented (Chiasson et al., 2016). It has also been observed that during the critical periods of brain development, if the brain is overstimulated it can have massive impacts on the brain development resulting in children having sleep disorders, depression, and anxiety. Studies have also shown that an overstimulated brain, at the time of its critical development, can lead to adverse effects including hyperactivity in adults (Lima.J.D.S., et al, 2021).

Cyber space has seen to have many psychological effects on children exposed to screens. Research suggests that limiting screen time can help to reduce loneliness and depression. (Hunt. G.M., Marx. R., Lipson.C., & Young.J., 2018).

The physiological functioning of the brain has changed ever since the fourth industrial revolution and is a cause for great concern. The effects are increasing by the day and the resulting developments are alarming. The effects have been so obvious in children that the WHO published guidelines to be strictly followed regarding allowable for children. This was also implemented in schools where it was observed that screen time had considerable effects on the working memory, afflicted various psychological problems, language developmental issues and the level of text comprehension of reading on the screen.

It is seen that about half of the mental illnesses begin around the age of 14 to mid 20's (Kessler et al., 2007) with anxiety and personality disorders beginning by the age of 11. (OECD,2012). With children growing up in the digital era, the majority of the children have been glued to their personal electronic gadgets, which means an open access to the internet which is usually without parental supervision (OECD, 2017).

Since the COVID-19 pandemic hit the world, people have been seen working from home and connecting through the internet for work, shopping, schools and even appointments for doctors including psychiatrists. With this evolving cyberspace regime, cybercrime has also been observed to evolve in tandem – the ensuing stress has had serious impacts on the mental health of individuals.

Psychiatrists should equip themselves with expertise to mitigate the potentially harmful effects of cybercrime on mental health of individuals. The ever-advancing trends in technology that are seamlessly integrated into modern living due to its innumerable benefits aren't without certain

repercussions and costs. Such drawbacks need to be handled tactfully to maintain an equilibrium between comfort, necessity, and associated risks. Technology these days has advanced and where it provides many benefits, it can also have its drawbacks that should be kept in mind. Awareness programs need to be conducted to educate people from a broad spectrum of the society about cyberspace and cybercrimes (Monteith. S., & Bauer. M et al., 2021)

Mental Health Effect on Cyber Practitioners and Victims

Cyberspace, driven by information systems and the Internet, is changing our world in unprecedented ways by facilitating economic development and creating innovative ways for people to communicate, engage, negotiate and collaborate with one another. Today's global economy is heavily reliant on cyberspace technology, as most facets of everyday human life depend on its proper and successful operation to succeed and flourish. There is almost no aspect of human endeavor that has not been domesticated in the realm of cyberspace. Personal and societal changes are brought on by cyberspace. The number of human events that have shifted from actual, face-to-face meetings to interactions facilitated by remote, distant connectivity has increased dramatically, changing human behaviour, goals, governance, parenting, and so on. The wellbeing of cyberspace, like public health, has an effect on about every area of contemporary culture. Businesses, governments, and societies would be unable to survive if critical elements of the cyberspace system are compromised or lost (Hinduja & Patchin, 2010). Failures in cyberspace health may have a huge impact on a nation's strength.

According to Centers for Disease Control and Prevention (CDC) cyberbullying has grown into a "public health epidemic" that cannot be overlooked. It is not only more serious than conventional bullying because cyberbullies will threaten victims across a number of mediums at any moment, but it has also been shown to frustrate juveniles' emotional, mental, psychological, and social development. According to National Crime Prevention Council (2007) more than forty-three percent of adolescents and adults report being victimized by cyberbullying. According to the Cyberbullying Research Center, people have now fully adopted online social networking. In the fall of 2009, seventy-three percent of teens aged twelve to seventeen used those sites or pages, up from fifty-eight percent in 2007. The persistent association between adolescents leads to cyberbullying's negative aspect on their mental health. In 2004, the Centers for Disease Control and Prevention (CDC) identified a significant trend in total suicide rates and found that female aged 1-14 years represented the greatest percentage increase in suicide rate from 2004 to 2004 (75.9%). Since then, suicide rates among young adults continue to cause national concern, with cyberbullying as a driving force. The syndrome has been dubbed "cyberbullicide" by researchers, who define it as suicide that is motivated indirectly or explicitly by encounters of online violence. Cyberbullying can have a negative impact on mental health, and there is a link that goes beyond that.

Researchers reported that cyber victim’s shows serious psychological harm such as higher level of depression, low self-esteem, poor-academic performance, anxiety, concentration and behavioral problems, alienation, violent behavior, suicidal intentions and even physical harm (Albin, 2012).

Over the years, the safety and security of cyberspace is challenged by criminal mind people. Criminal or hostile actions are an emerging challenge for society. Cyber-security tries to keep overcome this thereat with huge spending on research and development. As we depend more on technology to handle and sustain our daily lives, our susceptibility to cyberattacks increases, especially as many people work and learn from home during a pandemic. Simultaneously, the power of these cyberattacks is increasing. Hackers can now not only steal our credit card information and listen in on

private conversations, but they can also cause us physical harm. The scope includes: injecting fake data or malicious programs into information systems; stealing important data or programs from a system, or even seizing control of its operation; manipulating a system's output by altering data or programs, adding communications delays, and so on; and disturbing a system's performance by triggering irregular behavior or breaking data or programs.

Victims of identity theft report significant emotional distress, including anger, stress, depression and many physical symptoms. Victims of online love scams who experience the loss of a relationship report depression, feelings of guilt, deep shame and embarrassment. Heavy financial burdens have been associated with an increase in suicide attempts. Those with a history of mental health problems have an increased risk of psychological effects of the pandemic, especially adolescents and adults. People with anxiety and mood disorders experience severe pandemic-related anxiety and psychological problems are reported as well as insomnia. Pandemic stress increases alcohol and substance consumption.

Mental health has a critical impact on professionals in the industry and influences cybersecurity practices. In fact, the two are more related than you might think. Depression, burnout and suicide are becoming increasingly common among cybersecurity experts. Stress, depression and anxiety can lead to erratic impulses. These impulses manifest in various forms and can be used to justify extreme behavior such as data theft or destruction of systems.

One of the many side effects of work-related stress is that cybersecurity experts are particularly vulnerable. Over time, the problems of persistent stress, as experienced by cybersecurity experts, will become more serious. Indeed, the mentally ill are among the most at risk of suicide. This increased stress can lead to severe mental health problems with dire consequences.

Their sleep is disrupted and their energy levels drop. The consequences can be severe bouts of depression, anxiety and post-traumatic stress disorder. Victims struggle with feelings of powerlessness and vulnerability. In extreme cases, data theft can ruin lives.

Consumers are not alone in being harmed. Almost 85% reported trouble sleeping, 77% reported increased stress and 64% reported difficulty concentrating. Pain, headaches and cramps were also symptoms (57%). Half of the victims said they lost interest in activities and hobbies that they enjoyed.

The Internet is at the heart of our way of life among children and adolescents. While it opens up many positive perspectives in terms of access to information, knowledge and communication, it also carries the risk of possible negative experiences, which can have serious consequences on an individual level.

Part 3: Economic Impact of COVID-19

The covid-19 pandemic was an unprecedented event which has shaken billions of lives across the globe resultantly referred to as the new-normal (Lallie, 2021). Apart from exponential impact on societies, the pandemic created a series of unique cyberattacks which affected economies all over the world. There was considerable increase in phishing campaigns, denial of service (DDoS) attacks, internet espionages, fake news and mis and disinformation, and ransomware attacks. It is noted that cybercriminals hacked systems for people working from remote locations due to lack of security protocols (Quade, 2020). Furthermore, social engineering attacks and honest mistakes made in new

workflows are the part of new potential risks (Simonovich, 2020). Firms have already accepted the Fourth Industrial Revolution (4IR) technologies for better service standards and improved efficiency, the Fifth Industrial Revolution (5IR) is also changing the global economic sphere (Goldberg, 2020).

During the covid-19, global systems were attached, stock markets have been crashed around the world and every aspect of global economy has suffered severely. The financial services industry was hit by ransomware and phishing scams (Khan, et al 2020).

The following section explains various cyberattacks perpetrated during the covid-19 and did hit the global economy.

Malicious Domains

Since the outbreak of the pandemic, the initial first month of Jan 2020 witnessed more than 4000 domains linked to coronavirus. Checkpoint Risk Intelligence reported that 3% of these domains were malicious and another 5% were suspicious (Khan, et al 2020). Cyber hackers have used these domains to get personal information and scam for heinous purposes. There were more than 86000 new and malicious domains were reported to be registered related to covid-19 during early months (WHO, 2021).

Denial of Service Attacks

There was spike of cyberattacks on governments and healthcare institutions during covid-19. Cyber criminals interrupted the communication channels of health care organizations and governments by overflowing the systems with millions of users at the same time (WHO, 2021). The Department of Health and Human Services US was hit by cyberattack which affected widespread damage, impacting business systems, email servers and admissions (White, 2020). The international Police Organization (Interpol) has alarmed that government and hospitals will be prime targets for cyberattacks.

Ransomware Attacks

World has seen the unparalleled amount of ransomware attacks on education, public institutions, and medical organizations. As the shift from traditional method of working to digital mediums, hackers began to target the emergency services believing these institutions can pay the ransom (Khan, et al 2020). The most widely used approaches include links, email attachments, and compromised credentials for infecting an information system. The novel ransomware named “CoronaVirus” was created and disseminated which had the ability to steal passwords, and encrypted data (Cook, 2020). The significant increase of Ryuk ransomware was seen as a targeted, and manual mostly launched through a multistage attack leveraged by TrickBot and Emotet malware. This ransomware actor got on surface in 2019 asking for million dollars ransoms from hospitals, government agencies and organizations.

Fake or Malicious Social Media Accounts

Social media platforms are an important tool to share information, images, video and knowledge sharing. Cyber criminals gained access to social media networks for evil purposes. There have been hundreds of fake Facebook accounts and impersonification which resulted in dissemination of fake

news. Similarly, hackers try to attack social networks as a delivery mechanism, which result in compromising in user's location, contacts, and business activities (Cook, 2020).

Mobile Threats

The proliferation of cell phones particularly smartphones have opened another open space for cyber criminals to create fake applications. During covid-19, a mobile application named 'CovidLock' was developed which was actually a ransomware which misrepresented to be made from Android app to track the Covid patients (Dixon, 2020). Later on, it was known as a fake application as it locked the users mobile and gave 48 hours to pay ransom else the credentials and personal data would be sold out on dark web.

A study was done which has shown that healthcare facilities were the most vulnerable service to cyberattacks due to its emergency handling nature. The WEF (2020) issued a release in which they stated that four new malware samples were developed every second globally. It was a clear indication how cybercriminals were operating at complex and sophisticated levels.

As the world is moving towards the use of ubiquitous technologies, it needs to be prepared for cybersecurity measures and privacy issues too. With the recent wave of covid-19, the huge surge in cyberattacks were seen which will not come to an end sooner. In this regard, proactive policies and strategies are required to deal with such uncertainties and cyberattacks which not only have created negative ramifications on societies as a whole but also impacted the digital global economies.

Cybersecurity Practice

It has been seen that most organizations have poor cybersecurity practices and unprotected data in place, which actually make them vulnerable in times of uncertainties. In order to avoid cyber threats and attacks, organizations and governments should work on cybersecurity awareness campaigns and educational programs which can help them develop a cybersecurity culture and an echo system focusing on key components of governance structure.

In today's modern world, where data has become a strategic component of all activities of major actors of the digital economy, data governance is a key challenge for all the states. In 2015, the UN Group of Governmental Experts (GGE) meeting reached a consensus stating that sovereignty applies to the conduct by States of Information and Communications Technology (ICT), its related activities and jurisdiction over ICT infrastructure within the state. However, it did not provide any legal and clear consensus over the data resides outside the ICT infrastructure of state's jurisdiction. All states should interact with other nations to better understand and be aware of their legal position, encourage information sharing and bilateral and multilateral agreements to manage cross-border data flow.

Network and Wi-Fi Security

Another significant corroboration in this regard is unsecured WiFi networks at various locations. These WiFi connections may masquerade as legitimate WIFI networks, or have been comprised by bad actors prior to other participants connecting to them. Even if you are connecting thought a VPN, the connection ultimately connects to a compromised WIFI Network. There should be robust information security policies implemented by the organizations including extensive logging and monitoring policies and data access control. The configurations at both ends of every remote connection should be implemented in order to prevent prospective malicious use. Furthermore, employees should not have administration rights on organizations' owned systems.

Part 4: Social Impact

The worldwide pandemic has altered every segment of society. It has caused serious impacts on global social, psychological and economic wellbeing of every individual. The pandemic has resulted in serious demographic changes, world-wide unemployment, and closed down economic activities. It affected physical and mental health especially populations with lower social and economic status became victim of it. Higher stress and anxiety were seen amongst younger age groups, particularly females (Sarah, 2021). It has also caused psychological issues such as anxiety, depression and panic disorders. While the pandemic related stress has affected nearly everyone, it has long time impact on women worldwide (Almeida 2020).

The demographic and socioeconomic changes indicate that the pandemic has not affected every individual the same way (Collivignarelli et al. 2020). The various socioeconomic indicators such as rural or urban area, number of tenants in a specific household, education, gender, density of population are significant but the pandemic has mostly hit the poor areas (Messner 2020). The existing literature shows that areas with poor income were likely to be infected more than areas with higher income. The following are some of the factors which contributed to the socioeconomic change during the pandemic:

- Dense population posed challenge to social distancing in urban areas. In a household with more people could resulted in getting infected without much social contact.
- Different areas and regions have adopted different official policies for the virus. Office hours and advice varied from one region to another i.e. USA had different restriction policies between cities and states (Bashir et al. 2020).
- Working from home has benefitted social contacts with other people but this had better effects on only higher socio-economic jobs and limited number of people.
- People already suffering from chronic illness were at higher risk than normal and healthy people (Giannis et al. 2020; Zheng et al. 2020).
- Residents of lower socioeconomic conditions were at higher level of infection due to lack of healthcare services (Singh and Chauhan 2020).
- Studies suggest that women were particularly more affected with higher level of stress, depression, anxiety and post traumatic stress symptoms (Wang et al. 2020; Liu et al. 2020).
- Women have faced higher risks to intensify during pandemic such as severe environmental strain (Street and Dardis 2018), domestic violence (Campbell 2020), and depressive and anxiety disorders (Hao et al. 2020).
- For pregnant women, the pandemic brought higher level of increase fear and reluctance to visit doctors and deliver at hospitals.
- Working women have faced undue pressure since they were working from home, taking care of family and children, and performing her household tasks full time led to major mental health problems for them.
- Parents also faced a heavy load of stress which came in the form of online education. Many parents reported to be more anxious, fearful, agitated or depressed due to limited financial and social resources. Many parents started taking addictive substances and global sense of unpredictability remained obvious. This was substantial in case of parents with disabilities or single parents (Wang et al. 2020).

Part 5: Call for Actions

Mental health is a critical aspect of overall well-being; the World Health Organization has estimated that nearly one billion people worldwide live with a mental disorder, resulting in an annual global economic burden of $3 trillion. COVID-19 has only increased concerns about the general state of mental health, amid restrictive countermeasures that have isolated people from friends and loved ones.

Despite many pressing issues related to our collective state of mental well-being, only an estimated 3% of all global healthcare resources are directed at brain health.

The unprecedented events of covid19 have escalated the transformation world of digitalization, while some countries are undergoing digital transformation, some preparing for smart national project and some, paving way towards society 5.0, addressing societal challenges and becoming a sustainable, inclusive and human-centered society where both physical and cyber meet, it is important that we should have in place an international policy framework that addresses mental health and cyberspace. The paper presents call for actions at strategic level; organizational level; and technical level as below:

5.1. Strategic Level

5.1.1. Strong leadership

Government and Leaders should surround themselves with the right expertise instead of onboarding acquaintances to make up hiring numbers. A top-down governance model and culture are paramount to ensure the organization vision and roadmap are pervasive in the organization Leaders may also employ Business and IT champions in an integrated approach, where SIX SIGMA Green belts as one example would be part of the Cyber Culture.

5.1.2. Openness of Internet

Using a ‘smart contract’ to verify authenticity of the information before releasing on the news and having a decentralized based internet which allow user to fully control the data they shared should be adopted.

5.1.3. Data Sovereignty

Data Sovereignty should be seen as an inherent right of all world citizens in the Global Cyber Citizens Charter. Identity plays a critical role across many sectors and society. While there have been many attempts at a single identity provider, the proper technology was arguably not available in an immutable global solution. Built in a centralized manner, a true global identity solution gives too much power to a single entity, and leaves many at risk for data theft and fraud. The use of right technology such as Decentralized Ledger Technology where information is decentralized and tamper proof, allowing civilian to secure their own identity should be adopted.

5.1.4. Regulatory on AI

Regulation is considered inevitable to both encourage AI and manage associated risks. Regulation can minimize the risk of adverse and discriminatory impacts resulting from the design and application of automated decision systems.

5.1.5. Data Governance

In today's modern world, where data has become a strategic component of all activities of major actors of the digital economy, data governance is a key challenge for all the states. In 2015, the UN Group of Governmental Experts (GGE) meeting has reached on consensus stating that sovereignty applies to the conduct by States of Information and Communications Technology (ICT), its related activities and jurisdiction over ICT infrastructure within the state. However, it did not provide any legal and clear consensus over the data resides outside the ICT infrastructure of state's jurisdiction. All states should interact with other nations to better understand and be aware of their legal position, encourage information sharing and bilateral and multilateral agreements to manage cross-border data flow.

5.1.6. Gender Gap

There is a significant gender gap in cybersecurity, according to the ISC-2 Cybersecurity Workforce Study 2019, women make up just over a quarter (24%) of cybersecurity workers, compared to the early 2010s.

There are currently 4 million cybersecurity vacancies in the US and UK, worth $107.7 billion (€287 billion). That figure would rise to $138.1 billion (413 billion euros) if the number of women in cybersecurity matched that of men. There is a skills shortage in cybersecurity, and it needs to grow by 14.5% to meet current global demand.

Agency and leaders should encourage, promote, educate, elevate, and empower women as leaders and as a board member. This will balance the inequality and closes the gender gap. Research has shown that females have the ability to focus in a multi take mode, whilst bring positive views to the organization. There have already been extensive research where blended Gender cultures provide harmonized views, that are suited to put people as a priority and therefore creating positive business outcomes.

5.1.7. Mental Health

Mental health is extremely important for the sound functioning of an individual. As much as we pay attention to being physically healthy, keeping our minds healthy is equally important. Our mental health directly effects the physical health, and many mental disorders have physiological symptoms.

With ever advancing technology and the pace at which cyber space has occupied center-stage in our lives, it is extremely important to make sure that it does not negatively affect our mental health. Considering that ever since the corona virus pandemic hit the whole world, everything has been digitalized, from work, to schools, to appointments with doctors and shopping, the implications of navigating through cyber space without much oversight warrant a serious deviation from present usage routines.

Excessive reliance on digitalization is affecting the human brain, with relentless working regimes blurring the lines between work and private lives entailing over exposure to screens and, consequently, over stimulating the brain, leading to serious clinical and psychological disorders. This is particularly affecting children as their brains are in their early developmental stages where neural connections are formed, aiding in the development of various parts of the brain in a healthy way, a process which is now being impeded by the relentless and sustained intrusion of digital devices in their lives.

As much as it is important to go with the flow and become tech savvy – a mandatory requirement for most in this era - it does take a toll on the mental health of people. Many people, who, previously, were not well equipped with the tools of the digital world, had to learn from scratch. Shifting from physical offices and schools to work from home and online schooling, it has been a drastic change for this generation. Almost everyone has a personal electronic device, be it a cellphone or a tablet, desktop, or a laptop – not as items of luxury or hobby but more of a necessity.

Apart from physical (medical) repercussions of technology, there is a dire need to address psychological issues emanating out of extraneous threats such as cyber bullying. This is particularly hard for the new generation, where youngsters with impressionable minds have been exposed to the digital media from a very tender age. A concerted effort must be made to educate them about safely navigating digital media especially with reference to the internet and how to save themselves from cyber bullying. Often, cutting down screen time is thought to be a remedy enough for containing digital media related psychological issues, but neither is it a pragmatic approach, since defining an upper limit for such exposure is subjective and impractical for most, nor does it serve to counter cyber bullying effectively.

In the fourth industrial revolution almost, everything is accessible with a single click and is so fast paced, it has made human life extremely robotic. People have no choice but to keep up with this pace, or risk being left behind – a factor that triggers anxiety of disturbing proportions. Mental health practitioners need to put out content that can enable people to manage such strong emotions without letting technology get overwhelming. Psychiatrists should be equipped with relevant information regarding the cyber space and how cyber bullying occurs and how crimes are being carried out. People who become victims of such bullying develop mental disorders such as depression, anxiety etc. It is, therefore, imperative that a potent system is carved out with inputs from key stakeholders, taking into account academic studies and surveys, that could serve as an impetus towards drafting an effective counselling methodology taking a holistic view of all the factors playing a key role in effecting mental health of individuals across a broad spectrum of the global populations.

5.1.8. Psychological support on mental wellness

A call on non-biases treatment and therapy through arts, technology and holistic approaches focusing in balancing mental, physical, spiritual and emotional.

Mental wellness has become a critical component to the success of an entity – organization / country. Mental wellness is not just an occasional massage, it is a daily practice that leads to a whole life of the Self. Sleep is a vital area for health and well-being. Good self-esteem, health, body image, food and exercise are all big parts of an overall mental health and well-being.

Leaders should re-look at their existing strategies, policy and framework on mental wellness. They should reach out, support and to protect staff as much as possible from chronic stress and poor mental health. An ideal wellness framework should consist of occupational psychologist intervention such as a business / cyber psychologist, as well as practice of holistic regime.

5.1.9. Affect on the Cybersecurity Community

The CyberSecurity Community at large also are people and face mental health attacks in various forms, a much overlooked aspect. In an article published on InfoSecurity, Patrick Putman writes that cybersecurity professionals and criminal hackers have the same skill sets , many with similar

backgrounds, and their fundamental differentiator is their mental state. This makes for very interesting reading indeed.

As declared by the author , “What separates the good from the bad more than anything is empathy. It prevents professional hackers and social engineers from crossing the line.” According to the author, stress, depression, and anxiety are key factors in determining the mental outcome of the individual. There are several studies and evidence indicating the rise of mental illness among cybersecurity professionals. Ultimately there needs to be in organisation a Cyber-Socio culture where individuals received clear and professional support, this is not a HR function or human resource function by a deeper psychological function.

There needs to be a world standard, similar to the United nations where a layered governance model is devised that translates into real local geographical laws and regulations. This layer in turn in the onion of Cyber mental wellness has to be taken seriously by companies the Cyber mental well being culture. We would advocate a CCMHO-Chief Cyber Mental Health Officer, whose role is from top down and bottom up devise a support system that is driven by the board.

Finally, as a field, cybersecurity has an attraction for people of various backgrounds, on both sides of the so-called light and dark equation.. According to an article on Countable:

‘Anecdotal evidence suggests high prevalence of mental illness in the information security community, perhaps heightened by the hacker subculture attracting people from a variety of backgrounds, some of which may involve pre-existing mental health conditions.

Furthermore, cybersecurity attracts many ex-military members, who’ve had their own experiences with PTSD. These factors, among others, explicitly contribute to the increasing rate of mental health issues in the cyber workspace. Indeed, dealing with mental health issues was a recurring theme at the Black Hat USA conference for cybersecurity professionals in Las Vegas.

5.1.10. Accompanying Health Issues

Stress from work is often the cause of health issues. In fact, can greatly exacerbate existing medical conditions and lead to chronic disorders. For instance, stress can increase the frequency of varicose veins, as stress majorly weakens blood circulation. Heightened stress can rapidly increase blood pressure, which strains the walls of your veins. After a time of prolonged stress, such as that experienced by cybersecurity professionals, the problem can grow severe.

This is but one of the many side effects of work-related stress that cybersecurity professionals are vulnerable to. Heightened stress can also lead to severe mental health issues, which can have dire consequences.’ reference https://www.uscybersecurity.net/mental-health/’

5.1.11. Cyber Governance

Cyber Governance policies like GDPR for data protection should be devised. **CSP-**Cyber Social Protection should be an arm of the Cyber policy governments. Companies such as Google, Facebook, Twitter, should be governed globally by such a governance policy. This governance arm would in turn have real teeth, where fines and legal cases could be brought to bear on the social platforms.

The Legal framework has to be revised, to allow for **CCC**-Cyber Citizen Charter. This character would form part of organizations such as the UN, Governments and similar to the **Hague Convention.** The Hague convention is a series of international treaties issued from international conferences held at The Hague in the Netherlands in 1899 and 1907.Such an organization is already seen in several countries in several areas but requires global ratification.

5.2. Organizational Level

5.2.1. Human Centered System

Science and Technology should be jointly used to meet cultural, historical, societal and economic objectives. In this In this rapid fire digital economy, as we pave way towards society 5.0, organization should encourage human centered system such as flexi work arrangement while not taking away the benefits of an individual. The costs are minimal and the benefits are enormous. Employers will see an increase in employee attractiveness and retention, higher productivity and commitment, better work coverage, reduced absenteeism and a reputation for contributing to the integration of work and private life.

5.2.2. Education

Educators should consider implementation of Cybersecurity and Psychology studies from as young as primary school students. Research has found that depression can start from as early as the age of 11years old.

Moreover, world has seen the unparalleled transformation from traditional to digital mediums since the outbreak of the pandemic. In order to avoid cyberattacks such as social engineering, fake news and applications, cybersecurity protocols should be used. The educational protocols should be used by individuals and training protocols for the organizations. People working remotely should opt for VPNs in which strict information security policies should be used. It has been observed that organizations lacking in these protocols were more susceptible to cyberattacks during the pandemic as compared to organizations equipped with these protocols.

5.2.3. Mandatory of Policy Guidelines – NIST-800, ISO 27001, 27002, and 27005

There needs to be a stronger explicit guideline set that integrates into these policies, in order to get a holistic based approach, not multiple silo-based organizations and frameworks.

Cybersecurity awareness programs are key to educate and equip the organizations in finding potential threats and attacks. In this regard, organizations, governments and relevant agencies should work together vigilantly to combat cybercrimes amidst Covid-19.

5.2.4. Dark Web Governance

According to a recent Naked Security article, as the Dark Web is akin to the wild west of days past, so will the security change in the dark web as it did in the wild west. In the so-called light web we have DNS Serves, cloud environments, blockchain to determine source contracts as well as Digital certificates to validate sites. SIX governance areas on the Dark Web, according to the Global Commission on Information.

1.Mapping the Hidden Services Directory: Both TOR and I2P use a distributed hash table system to hide database information. Strategically deployed nodes could monitor and map this network.

2.Customer Data Monitoring: There will be no monitoring of consumers themselves, but rather destination requests to track down top-level rogue domains.

3.Social Site Monitoring: This includes watching over popular sites such as Pastebin to find hidden services.

4.Hidden Service Monitoring: Agencies must “snapshot” new services and sites as they appear for later analysis, since they disappear quickly.

5.Semantic Analysis: A shared database of hidden site activities and history should be built.
6.Marketplace Profiling: Sellers, buyers and intermediary agents committing illegal acts should be tracked.

5.2.5. Resilience Framework to Support Business Continuity

Business continuity is defined as the ability of an organization to continue providing products and services at a previously defined acceptable level after a disruptive incident. Business continuity planning or Business continuity and resilience planning is the process of creating systems of prevention and recovery to deal with potential threats to the company. An organization that resists failure is the ability to withstand changes in its environment and functions. Several Business Continuity Standards have been published by various standardization bodies to assist in the review of ongoing planning tasks.

One of the main differences between the resilience of companies and the standards for business continuity is the importance of anticipating and responding to potential disruptions. While both use risk management and other techniques to identify potential business risks, threats and vulnerabilities, the new standards reflect the need for further management processes that focus on corporate culture as part of an organization that can prepare for and prevent disruptive events.

Given the growing threat of disruption and attacks, the time has come for a dynamic response to disasters. This response must take the form of organizational resilience. Resilience must go beyond the management-oriented approach defined in ASIS SPC1 (2009) and the culture and practices of organizations defined in the guidelines published in ISO 22313. Instead, resilience goals across the organization's various disciplines must be improved, integrated, and coordinated - strategically, tactically, and operationally. Organizations must recognize that the management of business continuity must be a response to disruptions in order to continue operations at an acceptable and predefined level.

5.2.6. Cybersecurity Awareness Campaigns

It has been seen that most organizations have poor cybersecurity practices and unprotected data in place, which actually make them vulnerable in times of uncertainties. In order to avoid cyber threats and attacks, organizations and governments should work on cybersecurity awareness campaigns and educational programs which can help them develop a cybersecurity culture and an echo system focusing on key components of governance structure. Cybersecurity awareness programs are key

to educate and equip the organizations in finding potential threats and attacks. in this regard, organizations, governments and relevant agencies should work together vigilantly to combat cybercrimes amidst Covid-19.

5.3. Technical Level

5.3.1. Biometric Solutions

Biometric Solutions have evolved to a point where data sovereignty and ownership have become key factors in designing policy and solutions. Several companies are now providing KYS (Know your Stakeholders) as well as KYC (Know your customers). This is a flip on the use of Data and ultimately right of ownership. Several organizations have Cyber policies that touch up upon this such as NIST 800-53 ref https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final Security and Privacy Controls for Information Systems and Organizations.

The NIST 800-53 Cyber US Cyber Security standard focuses on IPDRR (Identify Protect Detect Respond Recover). The standard is more descriptive in nature and refers to such topics as **PR.DS-5:** Protection against data leaks is implemented. This data leaks PR.DS-5 could be extrapolated to and defined in more explicit terms such as Biometrics control of data.

With the Amplified and increased requirements for cyber dynamics, identity is a critical commodity that requires the highest level of cyber security. 'Physical biometric authentication alone cannot suffice for the sophisticated identity thefts emerging almost daily. And this calls for highly adaptive, Deep Learning Technology to be integrated with the existing verification solutions.'

5.3.2. Behavioral Biometrics

Behavioral Biometrics is one layer to identify and recognize patterns of user behavior that where variables are coded by AI into pattern recognition. Behavioral Biometrics uses Machine Learning, Artificial Intelligence, and Big Data to aggregate user interactions and creates a unique cyber-DNA for each authentic user. This method allows the behavioral identifiers, and Biometric applications to immediately recognize any change in user behavior. Behavioral Biometrics work seamlessly in real time, where the user remains protected and bad actor behavior is immediately flagged, with appropriate A.I. based response mechanisms.

The cutting-Edge Biometric solutions are now being built on the back of DLT 3.0, based on the Hash graph algorithm. This provides super low latency, a very lost cost to Crypto Tokenization compared to Bitcoin and Ethereum, whilst providing a bench-based Gossip Algorithm. The Immutable nature DLT, without the POW or POS requirements and where each node knows whatever other node knows, is the new DLT 3.0. Adding a Data Sovereign Biometric Wallet on top of this allows for: Trust Score, Self-Sovereign Identity, Selective Data Disclosure, Automation, **IVASS** (Identity Verification as A Service), Decentralization.

Ultimately this allows complete self-sovereignty whilst allowing governments and Organizations the ability to verify your identity without it being disseminated to third parties without the individuals consent. This provides a two-way KYC and KYS satisfying state and individual Cyber data protection Biometric requirements.

Conclusion

The Fourth Industrial Revolution is more than just having new technologies developed and introduced. It is a time of technological change, with a number of distinctive features that are associated with and simultaneous with broader societal changes. It led to changes that went beyond discrete technological possibilities and changed entire power systems. New technologies will make assets more durable and resilient, and data analysis will change the way they are managed. Physical products and services are enhanced by digital skills, thereby increasing their value. Consumers and businesses will be the customers at the epicenter of the economy, improving the way customers are served.

The spread of digital technologies will give the poor access to information, jobs and services that improve their standard of living. The Internet of Things (IoT) and blockchain will enhance data collection and analysis capabilities for more targeted and effective poverty reduction strategies. As new technology evolves, it brings new hopes to mankind but also threats and vulnerability.

In the social-Cyber world there need to be additional safeguards and mental wellbeing policies and regulation in place, that are akin to those by the financial regulators. Only when this is taken to this level and becomes a support and empathetic culture across business and social areas will we see a deep and beneficial societal change.

References

1. Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.
2. G., Rivest, R. L., Schiller, J. I., Schneier, B., Specter, M., & Weitzner, D. J. (2015). *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications* [MIT-CSAIL-TR-2015-026]. Massachusetts Institute of Technology. https://dspace.mit.edu/handle/1721.1/97690
3. Albin, K. A. (2012). Bullies in a wired world: The impact of cyberspace victimization on adolescent mental health and the need for cyberbullying legislation in Ohio. *JL & Health*, *25*, 155. Bullies in a wired world: The impact of cyberspace victimization on adolescent mental health and the need for cyberbullying legislation in Ohio. *JL & Health*, *25*, 155.
4. Almeida, M., Shrestha, A. D., Stojanac, D., & Miller, L. J. (2020). The impact of the COVID-19 pandemic on women's mental health. *Archives of women's mental health*, 1-8.
5. *Artificial Intelligence | Definition of Artificial Intelligence by Merriam-Webster*. (2021). https://www.merriam-webster.com/dictionary/artificial%20intelligence
6. Bada, M., & Nurse, J. R. C. (2019). The Social and Psychological Impact of Cyber-Attacks. *Emerging Cyber Tgreats and Cognitive Vulnerabilities*, 73–29.
7. Bashir MF, Ma B, Bilal, Komal B, Bashir MA, Tan D, Bashir M (2020a) Correlation between climate indicators and COVID-19 pandemic in New York. USA Sci Total Environ 728:138835. https://doi.org/10.1016/j.scitotenv.2020.138835
8. Bhat, C. S., Ragan, M. A., & Chang, S.-H. (2013). Cyberbullying in Asia. *Cyber Asia and the New Media*, *18*(2). https://www.asianstudies.org/publications/eaa/archives/cyberbullying-in-asia/
9. Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. *Journal of Cyber Policy*, *1*(2), 243–264. https://doi.org/10.1080/23738871.2016.1228990
10. Boulanin, V. (Ed.). (2019). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume I, Euro-Atlantic perspectives | SIPRI: Vol. I*. Stockholm International Peace Research Institute. https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic
11. Campbell AM (2020) An increasing risk of family violence during the Covid-19 pandemic: Strengthening community collaborations to save lives. Forensic Science International: Reports 2:100089. https://doi.org/10.1016/j.fsir.2020.100089
12. Chen H, Guo J, Wang C et al (2020) Clinical characteristics and intra- uterine vertical transmission potential of COVID-19 infection in nine pregnant women: a retrospective review of medical records https://doi. org/10.1016/S0140-6736(20)30360-3)
13. Chiasson M.A., Scheinmann R., Hartel D. Predictors of obesity in a cohort of children enrolled in WIC as infants and retained to 3 years of age. *J. Community Health.* 2016;41:127–133.
14. Collivignarelli MC, Abbà A, Bertanza G, Pedrazzani R, Ricciardi P, Miino MC (2020) Lockdown for CoViD-2019 in Milan: what are the effects on air quality? Sci Total Environ 732:139280. https://doi.org/10.1016/j.scitotenv.2020.139280
15. Cook, A., 2020, *COVID-19: Companies and verticals at risk for cyberattacks*, viewed 19 Apr 2021, from https://www.digitalshadows.com/blog-and-research/covid-19-companies-and-verticals-at-risk-for-cyber-attacks/.
16. D, S. (2020). Biometric Authentication, Access-Control and Encryption for Cyber Security and Privacy. *IITM*. https://www.academia.edu/7189542/Type_text_Biometric_Authentication_Access_Control_and_Encryption_for_Cyber_Security_and_Privacy
17. Dasgupta, D., Akhtar, Z., & Sen, S. (2020). Machine learning in cybersecurity: A comprehensive survey. *The Journal of Defense Modeling & Simulation*, 2020. https://doi.org/10.1177/1548512920951275
18. David-Ferdon, C., & Hertz, M. F. (2007). Electronic media, violence, and adolescents: An emerging public health problem. *Journal of Adolescent Health*, *41*(6), S1-S5.
19. Dixon, W. & Balson, D., 2020, *How COVID-19 shows the urgent need to address the cyber poverty gap*, from https://www.weforum.org/agenda/2020/03/covid-19-pandemic-shows-the-urgency-for-addressing-the-cyber-poverty-gap/.
20. Dong L, Tian J, He S, Zhu C, Wang J, Liu C, Yang J (2020) Possible vertical transmission of SARS-CoV-2 from an infected mother to her newborn [published online ahead of print, 2020 Mar 26]. JAMA. 323(18):1846–1848. https://doi.org/10.1001/jama.2020.4621
21. Eyre, H. A., Singh, A. B., & Reynolds, C. (2016). Tech giants enter mental health. *World Psychiatry*, *15*(1), 21–22. https://doi.org/10.1002/wps.20297
22. Fairhurst, M., Li, C., & Costa-Abreu, M. D. (2017). Predictive biometrics: A review and analysis of predicting personal characteristics from biometric data. *IET Biometrics*, *6*(6), 369–378. https://doi.org/10.1049/iet-bmt.2016.0169
23. Giannis D, Ziogas IA, Gianni P (2020) Coagulation disorders in coronavirus infected patients: COVID-19, SARS-CoV-1, MERS-CoV and lessons from the past. J Clin Vir:104362. https://doi.org/10.1016/j.jcv.2020.104362
24. Goldberg, C., 2020, *Cybersecurity and data privacy*, viewed 20 April 2021, from https://www.martindale.com/industry-group/goldberg-segalla-llp-5000609/Cybersecurity-and-Data-Privacy/.
25. Hao F, Tan W, Jiang L et al (2020) Do psychiatric patients experience more psychiatric symptoms during COVID-19 pandemic and lockdown? A case-control study with service and research implications for immunopsychiatry. Brain Behav Immun 87:100–106. https://doi.org/10.1016/j.bbi.2020.04.069
26. Hinduja, S., & Patchin, J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of suicide research*, *14*(3), 206-221.
27. Hunt.M.G., Marx. R., Lipson. C. &Young. J. No more FOMO: Limiting social media decreases loneliness and depression; Journal of Social and Clinical Psychology. 2018 ; 37:10
28. Hussain, F., & Qamar, U. (2016, April 25). *Identification and Correction of Misspelled Drugs' Names in Electronic Medical Records (EMR)*. 18th International Conference on Enterprise Information System (ICEIS), Rome, Italy. https://doi.org/10.5220/0005911503330338

29. Kessler, R. et al. (2007), “Age of onset of mental disorders: A review of recent literature”, Current Opinion in Psychiatry, Vol. 20/4, pp. 359-364.
30. Khan, N.A., Brohi, S.N. & Zaman, N., 2020, *Ten deadly cybersecurity threats amid COVID-19 pandemic*, IEEE, Researchgate publications, Berlin.
31. Kour, J., Hanmandlu, M., & Ansari, A. Q. (2016). Biometrics in Cyber Security. *Defence Science Journal*, *66*(6), 5. https://doi.org/10.14429/dsj.66.10800
32. Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248.
33. Lima.L.J., Cavalcante.A.M.O., Chagas.A.K.O., Leite. G.O., Campos. A.R. Audiovisual stimulation in childhood and adolescence promotes hyperactive behavior in adult mice. *Physiology and Behaviour*. 2021; 233
34. Lindert, J. (2017). Cyber-bullying and it its impact on mental health: Jutta Lindert. *European Journal of Public Health*, *27*(ckx187.581). https://doi.org/10.1093/eurpub/ckx187.581
35. Messner W (2020) The institutional and cultural context of cross-national variation in COVID-19 outbreaks. medRxiv. https://doi.org/10.1101/2020.03.30.20047589
36. Monteith, S., Bauer, M., Alda. M., Geddes. J., Whybrow.C.OP., & Glen. T. Increasing Cybercrime since the Pandemic: Concerns for Psychiatry: *Current Psychiatry reports* : (2021) 23: 18
37. National Crime Prevention Council. (2007). Teens and cyberbullying: Executive summary of a report on research.
38. OECD (2017), PISA 2015 Results (Volume III): Students' Well-Being, PISA, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264273856-en.
39. OECD (2012), Recommendation of the Council on the Protection of Children Online, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389 (accessed on 24 July 2018).
40. Poola, I. (2017). How Artificial Intelligence in Impacting Real Life Every day. *International Journal for Advance Research and Development*, *2*(10), 96–100.
41. Quade, P., 2020, 'A deep dive into the universe of cybersecurity: The digital big bang', World Economic Forum COVID Action Platform, viewed 22 April 2021, from www.weforum.org.
42. Qiu, T., Zhang, Y., Qiao, D., Zhang, X., Wymore, M. L., & Sangaiah, A. K. (2018). A Robust Time Synchronization Scheme for Industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(8), 3570–3580. https://doi.org/10.1109/TII.2017.2738842
43. Sabhnani, M. R., Rao, P. P., & Panchal, A. V. (2001). *AI Software in everday life: A Survey*. 5. http://www.cs.cmu.edu/~sabhnani/PDF/maics01.pdf
44. Saleh, Z. (2019). Artificial Intelligence Definition, Ethics and Standards. *The British University in Egypt*. https://www.researchgate.net/publication/332548325_Artificial_Intelligence_Definition_Ethics_and_Standards
45. Sarah J Barber, PhD, Hyunji Kim, MA, COVID-19 Worries and Behavior Changes in Older and Younger Men and Women, *The Journals of Gerontology: Series B*, Volume 76, Issue 2, February 2021, Pages e17–e23, https://doi.org/10.1093/geronb/gbaa068
46. Simonovich, L., 2020, 'Are utilities doing enough to protect themselves from cyber-attack?', *World Economic Forum*, viewed 22 April 2021, from https://www.weforum.org/agenda/2020/01/are-utilities-doing-enough-to-protect-themselves-from-cyberattack/.
47. Singh RP, Chauhan A (2020) Impact of lockdown on air quality in India during COVID-19 pandemic. Air Qual Atmos Heal 13:921–928. https://doi.org/10.1007/s11869-020-00863-1
48. Smith, R. G., & Eckroth, J. (2017). Building AI Applications: Yesterday, Today, and Tomorrow. *AI Magazine*, *38*(1), 6–22. https://doi.org/10.1609/aimag.v38i1.2709
49. Srividya, M., Subramaniam, M., & Natarajan, B. (2018). Behavioral Modeling for Mental Health using Machine Learning Algorithms. *Journal of Medical Systems*, *42*, 88. https://doi.org/10.1007/s10916-018-0934-5
50. Street AE, Dardis CM (2018) Using a social construction of gender lens to understand gender differences in posttraumatic stress disorder. Clin Psychol Rev 66:97–105
51. Stutzer, A., & Zehnder, M. (2013). Is camera surveillance an effective measure of counterterrorism? *Defence and Peace Economics*, *24*(1), 1–14. https://doi.org/10.1080/10242694.2011.650481
52. Thieme, A., Belgrave, D., & Doherty, G. (2020). Machine Learning in Mental Health: A Systematic Review of the HCI Literature to Support the Development of Effective and Implementable ML Systems. *ACM Transactions on Computer-Human Interaction*, *27*(5), 1–53. https://doi.org/10.1145/3398069
53. *What is Biometrics Security*. (2021, January 13). Www.Kaspersky.Com. https://www.kaspersky.com/resource-center/definitions/biometrics
54. White, K., 2020, *Life healthcare reports hacking attack*, viewed 20 April 2021, from https://www.businessday.co.za.
55. World Health Organization (WHO), 2020, *Beware of criminals pretending to be WHO*, viewed 20 April 2021,
56. World Health Organization. *Promoting mental health: concepts, emerging evidence, practice (Summary Report)* Geneva: World Health Organization; 2004.
57. Zheng YY, Ma YT, Zhang JY, Xie X (2020) COVID-19 and the cardiovascular system. Nat Rev Card 17(5):259–260. https://doi.org/10.1038/s41569-020-0360-5

Global Foundation for Cyber Studies and Research (GFCYBER) is an independent, nonprofit and non-partisan think tank, which conducts studies and research and provides consultation on cyberspace challenges and issues from the intersecting dimensions of policy and technology for the betterment of a globally-connected world. The foundation works on the philosophy that together we can secure the cyberspace!

Contact Us:

5614 Connecticut Avenue, N.W., No. 209,
Washington, D.C. 20015, USA.

www.gfcyber.org
info@gfcyber.org
@gfcyber