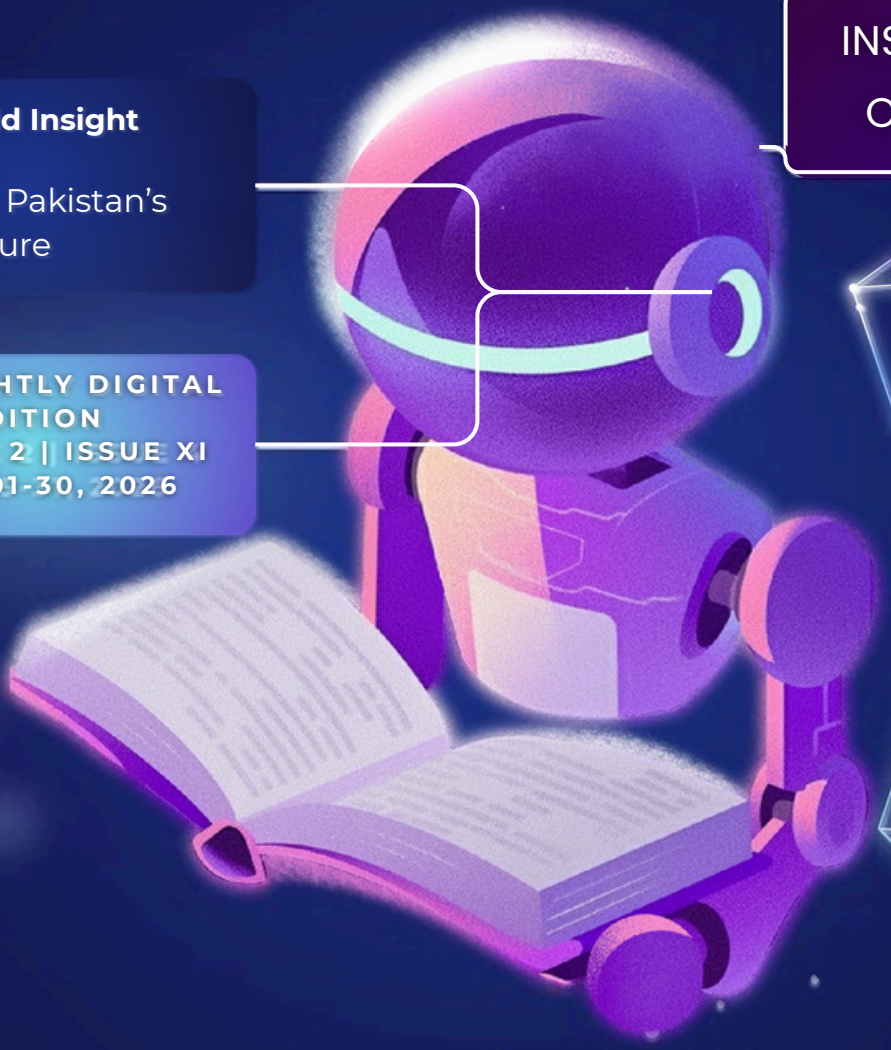
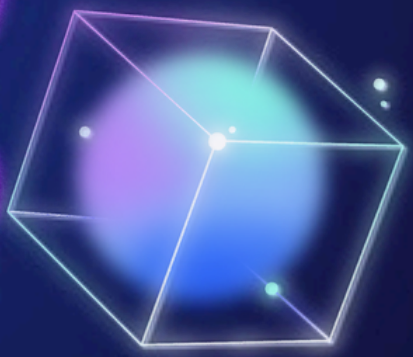
CYBER WORLD INSIGHT

INSIGHTS FROM OUR INTERNS

Cyber World Insight Magazine
Wired into Pakistan's Digital Future





FORTNIGHTLY DIGITAL EDITION
VOLUME 2 | ISSUE XI
JUNE 01-30, 2026

CYBERAGE MAGAZINE

FORTNIGHTLY DIGITAL EDITION |
DOWNLOAD PDF AT
WWW.CYBERWORLDINSIGHT.COM/MAGAZINE

CENTER OF CYBER WORLD INSIGHT

Shaping Pakistan's Digital Tomorrow

Volume 2 | Issue XI | June 01-30, 2026

About

CyberWorldInsight is a policy and ideas magazine dedicated to exploring how technology is transforming Pakistan's society, economy, and governance. We bring together voices from academia, industry, and policy to debate the opportunities and risks of the digital age. Our mission is to inform, challenge, and shape the national conversation on Pakistan's technological future.

Publishing Information

Cyber World Insight (CWi) ©2023–2025
The CyberWorld Insight Pakistan
Office #401, Omega Heights, E/11-3,
Islamabad, Pakistan
🌐 Website: www.cyberworldinsight.com
📧 Email:
magazine@cyberworldinsight.com
📱 Phone/WhatsApp: +92 333 5221408

Contributors

This edition features contributions from:

- CCWI Interns

Digital Edition

This is the Fortnightly Digital Edition of Cyber World Insight Magazine.
📲 Available online at:
🌐 www.cyberworldinsight.com/magazine
📥 Downloadable in PDF format for offline reading.

THE WAIT IS OVER!

YOUR JOURNEY STARTS NOW

CENTRE OF CYBER WORLD INSIGHT (CCWI)

RESEARCH • ANALYZE • EMPOWER

Be part of a **purpose-driven** internship that builds **skills**, inspires **impact** and shapes the **future**.

BATCH-II

SUMMER INTERNSHIP PROGRAM 2026

INTERNSHIP OPPORTUNITIES

RESEARCH DIVISION
Dive deep into research, analyze global issues and contribute to insightful reports.

CONTENT WRITERS DIVISION
Craft powerful articles, blogs and reports that inform and influence.

NEWS SECTION
Stay ahead. Report right. Be the voice of truth and awareness.

GRAPHIC & VIDEO DIVISION
Design visuals that speak. Create impactful graphics and videos that inspire.

CYBER SECURITY DIVISION
Explore, learn and strengthen the digital world through cyber defense.

ELIGIBILITY CRITERIA

For Research Division & Cyber Security Division

Minimum Qualification (at least):

- BS in Computer Science (CS)
- International Relations (IR)
- Defence & Strategic Studies
- Peace & Conflict Studies (PCS)
- Governance & Public Policy
- Or related disciplines

IMPORTANT DATES

LAST DATE TO APPLY
JULY 10, 2026

INTERNSHIP BEGINS
JULY 20, 2026

HOW TO APPLY?

1. Send your CV to hr@cyberworldinsight.com
2. Fill the Internship Application Form

SCAN QR CODE OR VISIT LINK BELOW

APPLY TODAY.

WHY JOIN CCWI?

- Work with experienced researchers and professionals
- Develop practical and professional skills
- Enhance your research and analytical capabilities
- Build an impressive portfolio
- Expand your professional network
- Receive a Certificate of Completion
- Opportunity to become part of future CCWI projects

CYBER WORLD INSIGHT

TABLE OF CONTENTS

PATRON IN CHIEF

It gives me immense pleasure to present Volume 2, Issue XI of CyberAge Magazine. This publication continues to promote thoughtful dialogue on cybersecurity, technology, artificial intelligence, diplomacy, education, and emerging global challenges.

We are living in an era where digital technologies are transforming every aspect of our lives. As cyberspace continues to redefine governance, economies, security, and human interaction, the need for informed research and responsible discourse has never been greater. This edition reflects our commitment to nurturing intellectual curiosity and providing a platform where emerging scholars and professionals can contribute meaningful insights to contemporary global debates.

I am particularly delighted to see the outstanding contributions of our authors, whose articles address some of the most pressing issues of our time, from women's leadership in cybersecurity and cyber diplomacy to cyber literacy, digital education, and the evolving role of artificial intelligence in cybersecurity.

I extend my heartfelt appreciation to our editorial team, reviewers, contributors, and readers, whose unwavering support has made CyberAge Magazine a trusted platform for disseminating knowledge. I hope this edition inspires critical thinking, encourages innovation, and motivates readers to actively contribute toward building a safer, more secure, and digitally empowered future. I wish every reader an enlightening and rewarding experience.

Patron in Chief CyberAge Magazine

Dr. Shabana Fayyaz

Message from the Chief Editor

Welcome to Volume 2, Issue XI of CyberAge Magazine. Every edition of our magazine reflects our commitment to publishing insightful, evidence-based, and forward-looking perspectives on the rapidly evolving cyber landscape. As technology reshapes international politics, business, education, and society, understanding these transformations has become essential for policymakers, researchers, practitioners, and students alike.

This issue presents a diverse collection of articles covering cybersecurity leadership, cyber literacy, digital diplomacy, online education, and the growing influence of artificial intelligence on cybersecurity. Each contribution has been carefully selected to provide readers with practical knowledge while encouraging meaningful academic discussion.

sincerely thank our talented authors for sharing their expertise and our editorial team for their dedication in maintaining the quality and integrity of this publication

We also turn our attention to the country's startup ecosystem and digital economy. Pakistan possesses an energetic and highly talented entrepreneurial community capable of driving innovation across multiple sectors. However, challenges such as inadequate digital infrastructure, regulatory uncertainty, limited access to investment, and inconsistent policy implementation continue to constrain sustainable growth. Unlocking the nation's digital potential will require a stable, supportive, and innovation-friendly environment.

Finally, no discussion of Pakistan's digital transformation would be complete without addressing cybersecurity. As cyber threats continue to evolve—from ransomware attacks and cybercrime to sophisticated state-sponsored operations—the need for robust cybersecurity has never been greater. Safeguarding Pakistan's digital infrastructure demands not only resilient defensive capabilities but also proactive national strategies that protect critical assets, preserve digital sovereignty, and strengthen resilience in an increasingly interconnected world.

This edition of Cyber World Insight is more than a collection of articles—it is an invitation to reflect on the strategic choices that will shape Pakistan's digital future. The nation can either remain reactive to global technological developments or embrace a forward-looking vision built on innovation, resilience, and responsible digital governance.

Chief Editor, CyberAge Magazine

Dr.Baqir Malik

Executive Editor's Note

It is our pleasure to present Volume 2, Issue XI of CyberAge Magazine, bringing together fresh perspectives on some of today's most significant developments in cyberspace and emerging technologies.

This edition highlights the importance of inclusive leadership, cyber awareness, digital diplomacy, technology-driven education, and the transformative impact of artificial intelligence on cybersecurity. These topics not only reflect current global trends but also emphasize the importance of interdisciplinary collaboration in addressing complex digital challenges.

The successful publication of this issue is the result of the collective efforts of our authors, reviewers, editors, designers, and the entire production team. Their dedication and professionalism continue to strengthen the quality and reputation of CyberAge Magazine.

We are grateful to our growing community of readers and contributors from around the world. Your engagement motivates us to continue providing a platform that promotes knowledge, innovation, and informed dialogue in the field of cybersecurity and emerging technologies.

Executive Editor, CyberAge Magazine

Jessica Avery

01 Women Leaders in Cyber Security

Author Intro

Anum Safdar Chishti
is a former intern at the Center if Cyber World Insight

Urgent leadership in strong cyber policy is needed as the digital world expands at an unprecedented rate. Governments, corporations, and billions of individuals are all affected by cybersecurity, making the presence of competent leaders more crucial than ever. The transformational leadership styles, resiliency, and unique perspectives that women bring to this field have long been required by the cybersecurity industry.

However, representation of women in cybersecurity remains low at all levels, from top decision-making positions to technical roles. Despite the existence of millions of cybersecurity experts worldwide, a small percentage of them are female, even as the demand for talent continues to grow. Women, representing an untapped pool of talent, can be seen as playing a pivotal role in closing this gap and strengthening global cyber resilience.

Why Women Are Key to Cyber Policy Leadership?

Network security and technical coding are no longer the exclusive aspects of cybersecurity. Policy thinking, communication, diplomacy, legal knowledge, and crisis management are all necessary. Ransomware and AI-driven attacks are just two examples of the modern cyberthreats that require leaders who can comprehend technology, analyze human behavior, and develop inclusive, long-term solutions. Women frequently provide a strong ethical emphasis, a collaborative approach, and people-centered problem-solving skills. In cyber policy, where decisions impact social systems, privacy rights, diplomacy, and international stability, these attributes are particularly important. Empathy, communication, flexibility, strategic vision, and the capacity to foster team trust are among the leadership qualities that senior women in cybersecurity have demonstrated. They empower talent, establish safe workplaces, and look beyond immediate gains. They are quite successful in intricate security settings because of these characteristics.

The Persistent Inequality in Gender

Despite advancements, only around 25% of cybersecurity positions worldwide are occupied by women. Although the pace of change is slow, forecasts indicate that improvement is expected. Women's entry, advancement, and retention in the sector remain restricted

Many of these obstacles are rooted in early experiences, such as the lack of female role models, limited exposure to STEM, and the false belief that cybersecurity is a technical field dominated by men.
Additionally, difficulties are encountered by women at work, including:

- Undervaluation of technical proficiency
- Prejudice in employment and advancement
- Pay disparities
- Absence of sponsorship and mentoring
- Isolation in male-dominated settings
- Insufficient visibility of professional paths

These barriers contribute to the persistent talent shortage by deterring women from entering the sector and forcing many to leave in the middle of their careers.

Barriers on the Leadership Journey

Common experiences for women advancing to executive positions in cybersecurity include gender bias, microaggressions, and presumptions about their abilities. Career advancement is continuously impeded by these obstacles, whether they are overt or covert.
Typical obstacles to leadership include: being overheard or disregarded during technical conversations; having expertise questioned; being neglected for important tasks; encountering challenges in advancing to executive positions due to the "glass ceiling"; being assigned leadership positions only under dire circumstances with a high chance of failure, resembling the glass cliff. Experiences of isolation, lack of networks, and navigating workplaces that require constant demonstrations of worth have also been reported by women executives. Nevertheless, resilience, wise decision-making, and the formation of supportive networks enable many women to overcome these obstacles and attain leadership positions.

The Influence of Sponsorship, Mentoring, and Reliable Networks

A frequent theme noted by women in cybersecurity leadership is the transformative impact of connections. The growth of abilities, self-assurance, and professional identity is fostered through mentoring. However, executive jobs are often made possible by sponsorship, where active support is provided to an individual by a senior leader.
According to female leaders: the most potent factor propelling them into senior roles was identified as sponsorship; safe spaces for learning and development were created through informal mentoring; new opportunities were discovered through relationships and industry gatherings; and advice was offered by trusted advisors during tough choices and stressful situations. Through these connections, prejudice was overcome, organizational politics were negotiated, and visibility in powerful circles was increased by women. This demonstrates that to increase the number of women in cyber leadership, defined channels must be provided by companies rather than relying solely on talent to emerge.

Global and Regional Initiatives Supporting Women

Several initiatives are currently being implemented to reduce the gender gap in cybersecurity and strengthen the leadership pipeline.

Women4Cyber and European Union Programs

Dedicated programs have been launched by Europe to support women through training, mentorship, scholarships, and networking. Initiatives such as Women4Cyber and Girls and Women in Digital aim to identify barriers, provide strategic policy guidance, build networks, and increase participation in cyber and ICT roles. These programs acknowledge that structural changes are required to address the gender gap — not just individual effort. Their approach demonstrates how coordinated public policy can support inclusion and empower future cyber leaders.

Women's Leadership Capabilities in Cyber Policy

Several characteristics frequently emerge from the lived experiences of women in cyber leadership:

- Vision for Strategy: A common focus on long-term thinking is found among female leaders, who align organizational and societal impact with

technical solutions.

- Cooperation and Diversity: A strong emphasis on collaboration, a range of viewpoints, and honest communication is placed within their leadership philosophies — all of which are essential in complicated cyber risk contexts.
- Making Ethical Decisions: Transparency, trust, and ethical security measures are often prioritized by women.
- Flexibility and Crisis Handling: A great capacity for leadership in times of uncertainty has been demonstrated by women in cybersecurity, particularly when new threats are being managed.
- Talent Empowerment: Teamwork is effectively fostered, potential is developed, and work environments that encourage creativity are established by them.

The Next Wave of Female Cyber Leaders

To increase women's engagement in cyber policy, real initiatives are needed across education, industry, and government.

What businesses can do: sponsorship initiatives should be created; clear channels for promotion should be established; microaggressions and unconscious bias should be addressed; flexible working circumstances should be established; the prominence of female role models should be boosted; women should be promoted to strategic roles, not merely supportive ones.

Conclusion

To create a more secure and resilient digital future, female leaders in cyber policy are crucial. Their experiences, viewpoints, and leadership philosophies provide harmony to an industry that has historically lacked variety. In addition to being an issue of equality, empowering women is strategically essential for global cybersecurity. Women are using creativity, empathy, and integrity to change the cyber landscape in a variety of ways, from executive decision-making to policy formulation. The next generation of cyber leaders will be more inclusive, varied, and capable of safeguarding our increasingly interconnected globe if obstacles are removed and opportunities are increased

STEM pipelines and scholarships should be increased; collaboration with business should occur to update the cyber curriculum; awareness efforts aimed toward young women and girls should be started; uniform standards for gender inclusion in all cyber environments should be established.

What female professionals are capable of: sponsors and mentors should be sought; participation in leadership networks and online communities should occur; voices should be raised, knowledge should be developed, and visibility should be asserted; more women should be encouraged to pursue careers in the field.

02 The Importance of Cyber Literacy for the Digital South:

Why should Pakistan and its Neighbouring Economies Act Now?

Bibi Ayesha Sadat
is an Afghan Student of International Relations at Quaid-i-Azam University.

In Pakistan, the use of digital devices and apps has become common now. We might check our bank app, chat with our loved ones on WhatsApp, or watch reels on Instagram. But have we ever thought about how safe we are online? Can our data and our privacy be at risk just because we missed a simple cyber-safety step?

In the digital age, almost everything we do is online. This makes our life much easier, but it also brings many risks that many people are unaware of it. For instance, threats like data theft and scams can happen to any individual in today's world. Therefore, cyber literacy becomes a survival skill in the digital age. Also, in countries like Pakistan, Afghanistan, and other South Asian countries, cyber literacy is a must-have skill for economic growth and national progress.

What is Cyber Literacy?

Cyber literacy is beyond being able to use digital tools. It is the skill of using technology safely, effectively, and responsibly. Moreover, cyber literacy teaches us how to protect our privacy, identify cyber threats, and behave ethically online.

In most developing economies, including South Asia, digital threats have become a common phenomenon. This has affected the economy. Thus, in South Asia, the understanding of cyber literacy is mandatory for the protection of personal data.

Why is Cyber Literacy important in South Asia?

Rapid Digital growth: In Pakistan and its neighbouring countries, we can witness rapid growth in the use of the internet and mobile phones. Nowadays, people from rural areas have access to the internet and digital devices. However, the problem is that in such cases, data safety is not prioritized. Data from developing economies shows that while access to digital tools improves, the skill to use them safely remains far behind. As an example, low-income countries are less skilled in the use of digital skills.

Localized System Weaknesses: In South Asia, we can see additional challenges. This is because many schools and educational institutions have limited resources. And small businesses can't afford cybersecurity measures. Also, some people use old versions of mobile phones that may be insecure. All these challenges lead to cyber threats. However, with the help of cyber literacy, we can easily reduce the risk of cyberattacks.

Economic Stake is High: When online banking is used by people and businesses, it is crucial to stay safe online. For instance, if a small business in cities like Peshawar or Karachi is vulnerable to a cyber scam, the owner loses money, which can directly affect the local economy. In other words, digital tools are helpful when people know how to protect

themselves online. Otherwise, the local economy will suffer.

How Can Cyber Literacy Influence the Economy?

1. Protection of Small Businesses and Everyday Commerce: Suppose a shop owner in Peshawar is running a WhatsApp-based order system. If he fails to recognize a scam message initially, he will lose money. In the future, he might avoid going for online-based businesses. But if he uses cyber literacy, then a fake message can be recognized easily. This will help the business run safely.
2. Enhancement of Productivity and Inclusiveness: When people know how to use digital tools safely, they can participate in the digital economy more actively. For instance, a person living in a rural area can work for an international company without leaving their home. Students can take online classes and get an education at an international level. Also, local producers can sell their products online through e-commerce platforms. Cyber literacy reduces the fear of using technology. When people feel safe online, they will try more online platforms, start their own businesses, and take part in digital learning. As a result, it will increase productivity and promote inclusiveness.
3. Economic Loss Reduction: Cybercrime is more dangerous when the victims are small firms and people with limited resources. This can lead to economic stagnation when digital systems are seen as unsafe. Thus, for countries like Pakistan and their surroundings, building trust in digital services (mobile banking, online learning, and etc.) is crucial. Cyber Literacy can support this trust.

Barriers to Cyber Literacy

Two Key Challenges in South Asia:

- Insufficient Data and Measurement: In most cases, we do not have solid data of how many people in Pakistan or its neighbouring countries, know how to behave safely in online platforms. Globally the data for low income countries is limited.
- Training Gaps: Many training centers focus on how to use tools, not how to use them safely. Moreover, there are inadequate standard cyber literacy centers in South Asia.

Conclusion

In South Asia, digital access is improving rapidly. People can afford buying devices, mobile data is cheaper, and internet connections are getting better day by day. The next step is to make sure people use digital devices safely and ethically. This is only possible through cyber literacy. By practicing safe digital habits, people can protect themselves and their communities. Thus, Pakistan and its neighbouring countries, should focus on teaching cyber literacy. This will promote new ideas, innovations, and wider participation in the digital economy. Thus, it will give chance to small towns and rural areas to grow.

Cyber literacy is not just a skill, it is the foundation of digital citizenship. For Pakistan and its neighbors, investing in it today means securing the region's digital future.

03 Cyber Diplomacy: Negotiating in the Digital Battlefield

Sabahat Fatima Soomro **Author Intro**

In today's digital age, where modern digital technology dominates the world, Cyber Diplomacy empowers businesses, governments, formal communications, cyberspace, and security, to a level, where it safeguards national interests and promotes international strength. It is undeniable that the state-sponsored cyberattacks, and digital information have transformed the cyber world into a new era of Cyber Diplomacy.

Cyber Diplomacy has literally just become a new practice of managing international relations and global conflict throughout a digital policy framework, which includes shaping treaties, norms, and cooperative structures. The digital sphere has evolved into a new battlefield where states project their authority and defend their interests, from ransomware attacks on vital infrastructure to disinformation operations influencing elections. Cyber diplomacy, or the art of managing international relations in the digital era, is a result of this growth. Cyberwarfare, in contrast to traditional warfare, is characterized by ambiguity; it is frequently challenging to identify the attacker, and responses must strike a balance between diplomacy and deterrence. The conflict between internet freedom and sovereignty further complicates policy formation. Some nations prioritize online transparency and human rights, while others push for more stringent state regulation of cyberspace. The development of a cohesive international framework is hampered by this ideological gap.

Deep geopolitical divisions impede the development of a globally enforceable cyber treaty, notwithstanding advancements. States have different interpretations of data protection, surveillance rights, and sovereignty. While some support an open and interoperable internet, others have national control as their first priority. Governance attempts are further complicated by the unparalleled influence that non-state actors and private tech businesses hold in cyberspace. Cyber diplomacy must overcome these gaps in the future by promoting openness, establishing confidence-boosting policies, and enticing engagement from a variety of stakeholders, including governments, academia, the commercial sector, and civil society.

Today, Cyber Diplomacy is known for its usage of diplomatic strategies, tools, and negotiations for the rising issues of cyberspace, cybersecurity,ybersecurity and digital governance. Nowadays, countries realize that traditional old-school methods of handling Diplomacy alone cannot deal with the borderless and faceless nature of cyber crimes. With the rapid growth of cyber attacks, which may or may not be, in some ways, related and sponsored by the state governments themselves, there has been a call for the need for international cooperation, so they can create the norms together, with benefits for them, increase their goodwill, and promote respectable states' behaviour online.

According to the United Nations Office for Disarmament Affairs (UNODA), international cyber norms were created by the Group of Government Experts in 2004, so they can design and manufacture behavioural guidelines for cyberspace and cybersecurity for states all over the world. Since then, this concept has been extended to include everything and cybersecurity, such as, digital human rights, data security and sovereignty, and neutralisation of cross-border cyberattacks.

Emerging Cyber Treaties and Normative Frameworks

In order to modify international cyber behaviour, the UN GGE and the Open-Ended Working Group (OEWG) have proposed some norms, which are:

- The countries will not deliberately allow their area to be used in wrongful international cyber attacks.
- Countries should coordinate with other countries in building capacity and cooperate in investigating cybercrime acts.
- Countries should not be targeting other countries' strategic institutions and infrastructure.
- Countries should be incorporating cyber standards into the frameworks of international humanitarian law and armaments control that are currently in place.

Simultaneously, regional organisations have worked with remarkable steps; the European Union Cybersecurity Act (2019) created a unique and unified certification framework for digital attacks. Whereas the (2001) Budapest Convention on Cybercrime continues to be a key element of global cooperation in the fight against cybercrime. Establishing guidelines for collaboration in the investigation and prosecution of cybercrimes, the Budapest Convention on Cybercrime continues to be one of the most significant legal frameworks. Recent initiatives to elucidate the application of current international law to cyberspace include the Tallinn Manual (although non-binding) and the Paris Call for Trust and Security in Cyberspace (2018). Regional cyber plans that strike a balance between international cooperation and digital sovereignty are being developed by ASEAN and EU nations.

Also there are some combined agreements, including, Russia-USA cyber security dialogues and China-EU digital cooperation network, provides growing security that the cyber world needed, to maintain confidentiality and mutual Diplomacy in digital age for transparency and accountability aspects.

As countries compete to capitalise on the potential of digital technology, cyberspace has emerged as a new area of both innovation and security. From massive ransomware assaults to electoral meddling, the digital sphere has made it harder to distinguish between war and peace. States are utilising normative frameworks and cyber treaties, which are global initiatives to establish acceptable conduct, discourage malevolent acts, and foster collective security in the digital sphere, to solve these issues.

Humanity is attempting to establish order in the increasingly unstable digital world through the emergence of cyber treaties and normative frameworks. Despite their flaws and ongoing development, they set the foundation for a cyberspace that is safer, more collaborative, and more moral.

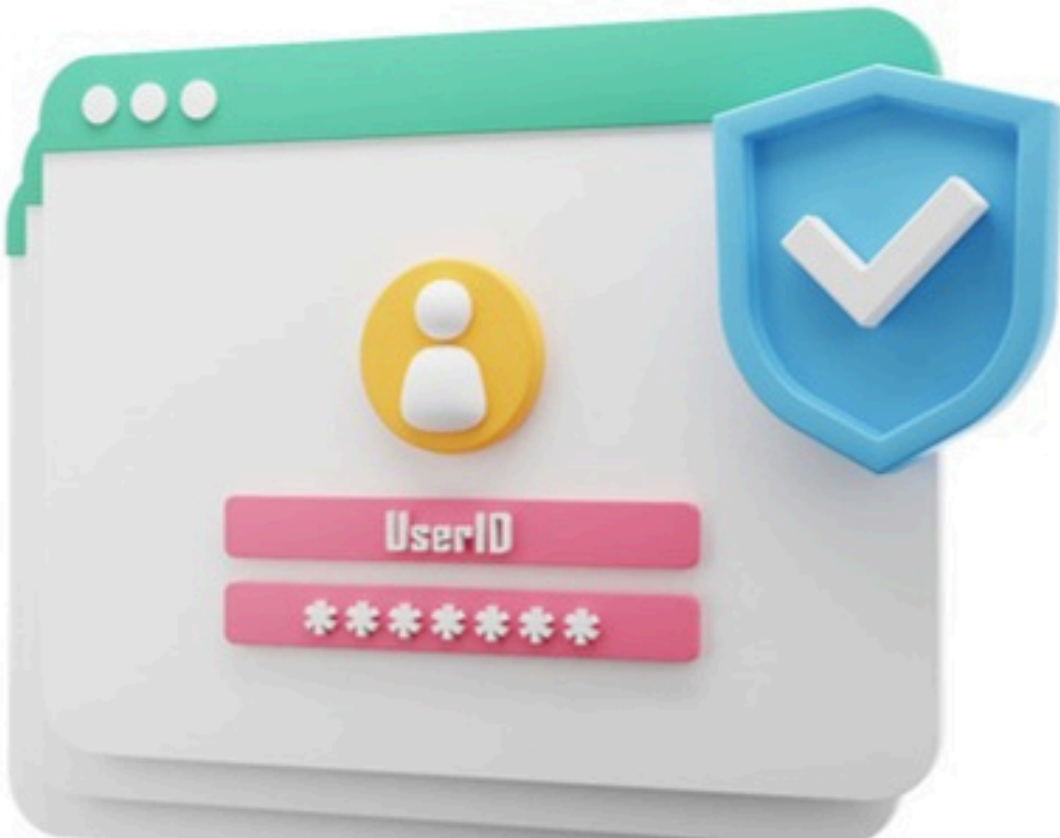
Conclusion

Despite its intangible nature, the digital attacks has real-world consequences. There is a ripping demand for strong cyber treaties and international rules as cyber crimes become more complicated. The future of global relations is represented by cyber diplomacy, a field where a country's power is determined not only by its military prowess but also by its capacity to lead, negotiate, and defend cyberspace. Since it is important to maintain world peace and stability in the twenty-first century, cyber diplomacy is no longer something you have an opinion on. Diplomacy in this connected globalised world, from handshake agreements to formal conversations, only to ensure that cyberspace is safe, open, and controlled by common rules and provides a safe space in the future. To maintain transparency, some basic steps are required to boost confidence, and ongoing communication between governments and IT stakeholders is necessary for cyber diplomacy to overcome these obstacles.

Some misunderstandings that could otherwise result in digital escalation can be avoided by creating crisis communication channels, encouraging cyber literacy among diplomats, and creating verification procedures for cyber norms.

Call to Action

We must invest in international trust, cybersecurity education, and diplomatic engagement to create a safer digital environment. After all, peace in cyberspace depends on our desire to work together. Because as technology develops, power dynamics continues to change its form, the digital age demands the countries for their collaboration, rather than their confrontation, in the Digital Battlefield. Countries must move past rhetoric and towards actual, enforceable agreements as cyber dangers continue to cross national boundaries. The ability of all of us to responsibly negotiate in the digital sphere may be more important for maintaining world peace in the future than military might.



GPU

04

WORLD CLASSROOMS, LOCAL IMPACT: HOW E-LEARNING CHANGES ECONOMIES GLOBALLY

Author Intro

Zarmeen Imran

Introduction

In our hyper-connected globalized world, e-learning is no longer a classroom variety of technology add-on but rather a sweeping movement that holds the potential to modify the nature of the way knowledge is shared, consumed, and even commercially exploited across national boundaries. Just imagine that due to mobile learning, AI-based individualization, and sleek immersive virtual classrooms, learners anywhere in the world can enter the high-quality process of education without caring about distance. Due to cross-border online learning expertise dissemination by universities, corporations, and online freelance educators globally has led to the introduction of cultural exchange, innovation, and acumen of competitive advantage in the international labour market. The results on the economy are enormous: a reduction in the price of education and an acceleration of skill formation in the new markets boost development by improving productivity. The students, especially in developing regions, now have access to the classes that were only provided in the prestigious institutions, and this brings everyone to a common level. Of course, the swifter the growth, the more it has to face digital divides, various regulatory conventions, and the ongoing search to achieve sustainable paradigms that combine accessibility and quality.

Finally, e-learning is defining the global economy that runs on knowledge, and which will, over time, redefine education and economic opportunity.

E-Learning: Full Steam Ahead

New technology has increased internet connectivity, and the emergence of an increased interest in flexibility has led to the e-learning market expanding at a much quicker rate than has been predicted by anyone. It is projected to

touch about 320.96 billion dollars by 2025, and by 2035, it is as big as 2.28 trillion dollars, which is a compound annual growth rate of 18.6%. The largest drivers are mobile learning (m-learning), the market growth of which is exceeding 23 per cent a year, and the recent popularity of artificial intelligence in the design of individualized learning journeys. AI has been used in the deployment of e-learning platforms within companies, such as the one implemented by Big Blue Inc. (IBM) to train its employees in all parts of the world at a faster rate, which increases productivity. One of the top global platforms, Coursera, received over 20 million additional learners in 2021 who were offered the courses in such elite academic institutions as the University of London and Stanford in over 190 countries.

Even the developing world is picking up. Back in Kenya, Eneza Education employs interactive lessons delivered as SMSs to students, even in remote locations, who do not even require smartphones or broadband. The above world trends in e-learning demonstrate that the Internet-based type of education is capable of growing and breaching the boundaries of national borders, which helps spread knowledge, drive innovation, and equip millions of workers to serve the constantly churning economy.

In the past 10 years, online education across states and virtual classrooms has transformed into a game-changer, facilitating the strengths of students and professionals to jump over walls of geographical and socio-economic divides that previously failed to provide students with an exceptional schooling. These platforms, courtesy of faster enhancements in the digital infrastructure, cause learners to access resources previously available only to developed countries, involving the use of digital infrastructure. Consider Coursera and edX, both providers work with heavyweight universities such as Harvard, Oxford, and the University of Tokyo, and are now offering fully accredited courses or certification programs as well as skill-oriented online courses to millions of students around the globe. Elsewhere, Coursera alone recorded over 20 million new registrations in the year 2021, and there was a marked increase in Asia Pacific, Europe, and Africa regions, where the most junctures of students were recorded to enroll at 43 per cent, the highest worldwide. In addition to the large names, there are niche organizations such as the African Virtual University and the Commonwealth of Learning Virtual University for Small States of the Commonwealth, offering region-specific, low-cost courses to meet local needs, which give power to the students in areas where there are few physical campuses. In the cultural arena, we have virtual exchanges like e-tandem language learning and collaborative research, whereas in the corporate world, we find giants like Google and Microsoft operating integrated e-learning systems that can train their staff across continents in real time, ensuring a uniform knowledge level. Overall, this synergy that correlates technology and education is not only access-expanding but also strengthens the human capital base of the world, which stimulates economic development in a knowledge-based economy. Nonetheless, challenges still exist, among them the most pronounced digital gap, a spotty domestic regulatory environment, and linguistic barriers that will have to be addressed should we bring the full potential of cross-border virtual learning to fruition.

E-Learning Impact on Economics

The influence of e-learning on the global economy is strong enough to influence productivity, construction of workforces, and even national developmental trends. Reducing the cost of education and training delivery through online learning allows individuals, companies, and governments to make better use of existing resources and afford access to significantly more people than could be achieved with traditional schools. Corporate research indicates that implementation of e-learning can cut down training expenditure by 40-60% and, in


LIVE
online
LEARNING

most cases, lead to high performance in addition to increased staff retention rates. Organizations such as IBM have cited that they have recaptured almost 200 million dollars a year in moving to digital learning platforms that enable employees around-the-clock access to training, any time and at any location that suits them. The impact is even larger in the developing countries; initiatives like Eneza Education in Kenya employ low-cost mobile education to provide rural students with basic skills that will make their employability and earning prospects sharper over the long term. At a macroeconomic level, e-learning is resulting in the workforce being more flexible and innovative something highly essential in the global market today, where it is fast changing. It allows generating sustainable economic growth through employing sectors that focus on IT, renewable energy, and healthcare activities, which can be upskilled rapidly due to an imminent rise in the applicability of emerging technologies. Online education across national boundaries also fuels educational services across national markets that add billions of dollars to universities and educational technology supply firms, and employs content developers, instruction designers, and specialists in electronic infrastructures.

Nevertheless, the economic opportunities are also not equal; the areas that are poorly connected to the internet or have fewer devices at their disposal are left behind, which may increase the socio-economic disparities. To achieve the best value of e-learning to the economy, it needs to be coordinated to go along with policies that enhance digital inclusion policies investment in the broadband infrastructure, as well as ensuring equal access to high-quality content.

Strengths and Limitations in E-Learning

In the contemporary globalized economy, e-learning stands out due to its accessibility, flexibility, and the ability to provide high-level content to the learners in whichever location and at any given time, thus making it such a blessing to both students and professionals with several priorities to attend to. Studies indicate that e-learning could have an effect of increasing retention by 25-60 percent and the shortening of learning time to a maximum of 60 percent compared to face-to-face training, making it time and cost effective. The flow of technological innovation is increasing personalization, interactivity, and immersion in artificial intelligence, augmented reality, and virtual reality, even met averse-based classrooms. Indicatively, aspiring medical students or trainees would have the opportunity of getting lost in VR-based simulation of

surgical procedures without having to face the life-threatening risks involved, without the involvement of actual patients, and employees of companies could stick themselves in AI-enabled micro learning jigs where they are taught to improve their areas of weakness. There are, however, many obstacles still. Digital divide is fuelled by inequitable access to stable technology and the internet, especially in low-income and rural regions. Students can drop out of online courses relatively often, interaction with peers may be minimal, and the quality of the content varies across platforms. Even though some of these issues are sought to be mitigated by the emerging technologies, the high cost of implementation, as well as infrastructure requirements, might hinder implementation in developing countries, and thus, collective balanced strategies should be implemented to enhance e-learning on a global scale.

Conclusion

On the whole, e-learning in a global economy has emerged as a game-changer that has changed the way education is taught, received, and appreciated in all countries across the globe. It can break down physical and socio-economic boundaries, allowing learners who might have been on the periphery to experience high-quality education that can spark innovation, develop a workforce, and drive economies.

International platforms (such as Coursera and edX) and national ones (such as the African Virtual University) give millions more access to opportunities that used to be denied to a small group. The economic benefit of it is also prominent, as it cuts down the costs of training, accelerates the process of developing

skills, and opens up new markets for digital educational services. What may hold these goals back, however, are complications like digital divide, variable regulations, and infrastructure capabilities to handle the heavy workload? In the future, e-learning will require focused investments in digital access, inclusive content design, and an ever-more cross-border collaboration policy. By overcoming these obstacles successfully, e-learning will enhance not only the worldwide knowledge economy but also contribute to the creation of a more equal and more unified world.

05

The Artificial Intelligence Arms Race:

AI and Machine Learning are Transitioning the Face of Cybersecurity

Author Intro

Hajira Assad

is an undergrad student at SPIR in Quaid-e-Azam University. She can be reached at hajiraassad181104@gmail.com

Introduction: The New Digital Battlefield

In the contemporary globalized and digitalized society, the hurdle of cybersecurity is of great attention among individuals, organizations, and even states. The elevation of cyber attacks is increasing rapidly, with a great proportion and number, as cyber criminals are employing advanced techniques in identifying vulnerabilities in defenses. Even highly advanced digital ecosystems are not secured by the mere conventional, rule-based security platforms that utilize distinguished threat indicators and humans. In such a momentous setting, the most transformative aspect in the field of cybersecurity has been the creation of Artificial Intelligence (AI) and specifically, its sub-technology, Machine Learning (ML). It portrays the zenith of the period of reactive defense, making way for active, forward-thinking, and intelligent defense. Nevertheless, it isn't a one-sided coin; bad actors also have access to the same technologies, and an unending war of algorithms is making it difficult for the next generation of digital warfare

1. **Defensive Shield: AI as the Guardian**

AI and ML will enable security systems to go beyond an established collection of rules to tackle emerging threats in real-time. The technologies will be able to process vast amounts of information, so that patterns are formed, potential attacks are predicted, and a reaction is realized with minimized human interference.

High-Level Threat Detection and Anomaly Identification

Traditional antivirus software depends on known malware signatures, and this cannot operate with zero-day attacks and rising threats. Unsupervised learning models are certain types of ML algorithms that tackle the trap by supplying a baseline of behavior to networks and users.

They process large volumes of data, like network traffic, login times, file access patterns, and resource use, to identify the gradual and anomalous operation that signals a leak. Using the example of an ML system, a user downloading terabytes of information at 3 AM can be detected, or a server in one domain of the globe attempting to access a sensitive database in a different region, milliseconds apartThese actions will not be detected by traditional defenses provided by the perimeter, whereas is detected in real-time, allowing security personnel time to take action before it is too late.

For instance, one of the most successful AI-based cybersecurity companies, Darktrace, uses ML algorithms to forecast the behavior of all users and devices within a network. With deviations, e.g., when an abnormal data transfer occurs or in an

Anti-Phishing and Anti-Social Engineering Detection and Prevention

One of the most popular attack vectors is phishing, and cybercriminals will never cease to improve their techniques to swindle their victims. One part of artificial intelligence, which is now applied to search emails and messages and understand them like humans, is NLP. The linguistic hints, emotion, and setting: these models recognize the existence of superior impersonation attempts, urgency-driven scams, and intent despite campaigns that have never been witnessed. This ensures that such social engineering attacks have very low success.

> *Gmail is a Google email service relying on ML models to filter phishing messages with 99.9 percent precision. The system analyses millions of emails daily, learns new patterns, and adapts to the new threats, without the system operator ever having to update the system.*

SOAR: Automated Incident Response

The speed is critical when a threat is detected. AI-powered Security Orchestration, Automation, and Response (SOAR) platforms can run a pre-defined playbook in milliseconds. This includes: separating infected endpoints, blocking bad IP addresses, destroying user credentials, and activating backup facilities. The impact of this automation is that the dwell time reduces by a large margin and enables human analysts to devote time towards strategic threat hunting.

IBM QRadar SOAR is an artificial intelligence-based system that automatically reacts to common security threats, such as isolating malware-infected computers or blacklisting IP addresses with malicious traffic. This makes the response time only a matter of several seconds.

Predictive Vulnerability Management

ML can predict the weak areas of the system, which are the most likely ones to be exploited, as opposed to responding to them with patches. By tracking trends on forums in the dark web, previous attack history, and software settings, AI systems can prioritize what vulnerabilities are most likely to be fixed. This will help organizations to roll out their resources efficiently and close their borders before they are attacked.

Example: There is an API that uses ML to scan the vulnerability data and rank the patches by their potential exploit, named Threat Protection at Microsoft. This kind of proactive approach has helped organizations reduce their attack surface.

2. **The Offensive Sword: AI as a Weapon**

These AI applications have democratized and provided cybercriminals with new tools that enable them to organize more intricate and large-scale attacks.

AI-Powered Cyberattacks

Hyper-Realistic Phishing: AI-based programs such as OpenAI GPT-4 can create perfectly realistic, targeted phishing emails and deepfake audio messages. Different tools mimic the writing style of a CEO or the voice of a reliable colleague to authorize fraudulent transactions, and these are extremely hard to trace.

Evasive Malware: It is possible to create polymorphic and metamorphic malware using ML, which can automatically alter its code each time it infects the system. This makes it impossible to detect it by signature-based detection systems since the malware never resembles itself.

Password Guessing: AI can be trained to optimise brute force attacks by studying past passwords and generating possible combinations of passwords. This makes the process of cracking efforts highly successful.

Case in point: DeepLocker attack had already demonstrated the potential of employing AI to create extremely particular malware.

Automated Vulnerability Discovery and Exploitation

AI applications can automatically search through code, networks, and applications that people cannot search through at scale and speed. This will allow the attackers to detect and take advantage of zero-day attacks faster than the defenders can seal the holes.

Deepfakes and Fraud

Deepfakes or AI-generated fake media are a threat to corporate and national security on a serious scale.

Example: AI-generated audio was used to impersonate the voice of a CEO to make a subordinate pay 243,000 dollars in a false account.

3. **The Inevitable Arms Race and Its Problems**

Adversarial Machine Learning: AI training data can be poisoned by malignant units and develop inputs that are specifically intended to perplex ML models into wrongly grouping risky actions as innocent. As an example, changing a malware file by a few bytes can make it invisible to an AI-based scanner.

Data Privacy and Bias: Massive data questions can be posed, as AI models need massive amounts of data to work. Moreover, biased training information can result in risks not known by incorrect models for a given demographic or location.

The Skills Gap: Security launched and operated by robust AI needs very specialized skills, inducing a noticeable resource gap between firms and small organizations.

4. Case Studies

Deep Instinct: Global Case Study

Difficulty: Malware attacks must be avoided. Solution: Deep Instinct leverages a more powerful version of ML, where cybersecurity is deeply informed. The result is its trained program on hundreds of millions of malicious and benign files can warn and block malware it has never seen with incredible precision of accuracy and near-zero false alarms, before any file can run on an endpoint.

Pakistan Case Study: Banking Resilience

Problem: Pakistani banks, HBL and UBL among them, suffered cases of advanced transaction fraud and phishing scams. ML models review real-time transaction data and compare individual customer behavior patterns. Result: The systems are able to identify and block suspicious transactions in milliseconds. HBL reported a 30-percent-plus drop in successful fraudulent transactions following the implementation.

Pakistan Case Study: Securing Critical Infrastructure

Challenge: PTA had to secure the national telecom infrastructure against mass-scale DDoS attacks. Solution: AI-based system to analyze network traffic and detect abnormalities. Result: Automatic mitigation through traffic diversion and filtering before the attack can halt the system.

Conclusion

The future of AI and ML is not the silver bullet and transition of cybersecurity, but an evolutionary leap. It affirms a new formation of self-healing and self-adaptive security systems. Nonetheless, AI will not replace human analysts. The future, however, is in symbiosis. AI does the scale, speed, and automation of threat identification and response. Human beings have a strategic understanding of concepts and ethical judgment. The solution is to invest in homegrown artificial intelligence, government-business partnerships to support pivotal domains, and to establish a sound doctrine that would certify that such powerful technologies are used with constraint. Not only is staying up to date in the global arms race of algorithms a technological problem, but it is a national security tactical imperative.

“The Road Ahead”

At CyberWorldInsight, we believe technology is more than tools and trends

It’s the force reshaping how we live, work, and govern. Our mission is simple: to spark dialogue, share knowledge, and guide Pakistan toward a bold digital future