

## কলাম

মতামত

# বাংলাদেশের শিক্ষাক্রমে সাইবার নিরাপত্তা শিক্ষা যুক্ত করা সময়ের দাবি

লেখা: হিউ গিল

প্রকাশ: ১৭ নভেম্বর ২০২৫, ১৮: ৩৫



সাইবার নিরাপত্তা ছবি: ফেসবুকের সৌজন্যে

প্রযুক্তির ওপর মানুষের নির্ভরশীলতা ক্রমেই বাড়ছে; এর ফলে, একই সঙ্গে তৈরি হচ্ছে নিরাপত্তা ঝুঁকি, যা রাষ্ট্র, প্রতিষ্ঠান ও ব্যক্তিগত নিরাপত্তা, সবকিছুকেই হুমকির মুখে ফেলছে। ‘সাইবারসিকিউরিটি ভেঞ্চারস’-এর গবেষণা অনুযায়ী, ২০২৫ সালের মধ্যে সাইবার অপরাধের বিশ্বব্যাপী আর্থিক ক্ষতি বছরে ১০ দশমিক ৫ ট্রিলিয়ন মার্কিন ডলারে পৌঁছাবে।

এই বিপুল পরিমাণ ক্ষতির পূর্বাভাস প্রমাণ করে জাতীয় পর্যায়ে বাংলাদেশসহ দ্রুত উন্নয়নশীল দেশগুলোর জন্য সাইবার নিরাপত্তা বিষয়ে সচেতনতা ও শিক্ষা এখন সময়ের দাবি। সাইবার নিরাপত্তা জাতীয় উন্নয়ন পরিকল্পনার অবিচ্ছেদ্য অংশ হওয়া উচিত।

কৃত্রিম বুদ্ধিমত্তা (এআই) পণ্য, বাজার ও শিল্প খাতের বিকাশকে ত্বরান্বিত করছে। এমন প্রেক্ষাপটে সাইবার নিরাপত্তা বিষয়ে বিশেষজ্ঞদের চাহিদা আগের যেকোনো সময়ের চেয়ে অনেক বেশি। আধুনিক এআই-নির্ভর সিস্টেম বিপুল পরিমাণ তথ্য তৈরি করে, যার অনেকটাই সংবেদনশীল এবং সহজেই অপব্যবহারের ঝুঁকিতে থাকে। এসব সিস্টেম সুরক্ষিত রাখতে হলে বড় ধরনের ডেটার দুর্বলতা বুঝে তা মোকাবিলা করার জন্য পেশাগত জ্ঞান ও দক্ষতা থাকা অপরিহার্য। তাই সাইবার নিরাপত্তা বিশেষজ্ঞদের চাহিদা এখন পুরো বিশ্বজুড়ে দ্রুত বৃদ্ধি পাচ্ছে।

স্বাস্থ্যসেবা থেকে শুরু করে আর্থিক খাত, সব জায়গাতেই এইআইয়ের ব্যবহার বাড়ছে; সঙ্গে বাড়ছে সাইবার ঝুঁকির পরিধি ও ধরন। সিস্টেমগুলো এখন আগের চেয়ে বেশি ঝুঁকিতে রয়েছে। প্রতিপক্ষের আক্রমণ, তথ্য ফাঁস কিংবা পূর্বাভাসভিত্তিক মডেলের অপব্যবহারের আশঙ্কা বাড়ছে। এসব নতুন ধরনের ঝুঁকি মোকাবিলায় বিশেষ দক্ষতাসম্পন্ন মানবসম্পদ দরকার, যাদের কাজ হবে এই জটিল প্রযুক্তির দুর্বলতা শনাক্ত ও প্রতিরোধ করা।

এ প্রয়োজনকে অনুধাবন করে বিশ্বের অনেক বিশ্ববিদ্যালয় ও প্রশিক্ষণ প্রতিষ্ঠান ইতিমধ্যেই তাদের পাঠ্যক্রমে সাইবার নিরাপত্তা বিষয়টি অন্তর্ভুক্ত করেছে। যুক্তরাষ্ট্র এই ক্ষেত্রে সবচেয়ে এগিয়ে রয়েছে। তাদের ‘ন্যাশনাল ইনিশিয়েটিভ ফর সাইবারসিকিউরিটি এডুকেশন (এনআইসিই)’ শীর্ষক উদ্যোগ শিক্ষাপ্রতিষ্ঠান ও শিল্প খাতের সঙ্গে যুক্ত হয়ে দক্ষ মানবসম্পদ তৈরি করেছে, যারা এআই-নির্ভর ডিজিটাল অর্থনীতির জটিল চ্যালেঞ্জ মোকাবিলা করতে সক্ষম।

অন্যদিকে বাংলাদেশের অবস্থা এ ক্ষেত্রে অনেকটাই বিপরীত। এ চ্যালেঞ্জ মোকাবিলায় একদিকে যেমন শিক্ষাক্ষেত্রে যথেষ্ট প্রস্তুতি নেই, অন্যদিকে ব্যবহারিক প্রস্তুতিরও ঘাটতি রয়েছে। সাম্প্রতিক সাইবার হামলাগুলো এ দুর্বলতাকে আরও স্পষ্ট করেছে। উদাহরণ হিসেবে বলা যায়, ‘স্মার্ট এনআইডি’ ডেটাবেজ হ্যাকের ঘটনায় প্রায় পাঁচ কোটির বেশি নাগরিকের তথ্য ফাঁস হয়েছে। আবার ২০২৫ সালের শুরুতে এক শীর্ষ আর্থিক প্রতিষ্ঠানের তথ্য ফাঁসের ঘটনাও সীমিত প্রযুক্তিগত সক্ষমতাকে সামনে এনেছে। এ ঘটনাগুলো চোখে আঙুল দিয়ে দেখিয়ে দিয়েছে দেশে প্রশিক্ষিত সাইবার নিরাপত্তা বিশেষজ্ঞের ঘাটতি কতটা গভীর এবং কেন এ বিষয়ে আনুষ্ঠানিক শিক্ষার ওপর জোর দেওয়া জরুরি।

২০২৪ সালের ‘সাইবারসিকিউরিটি ওয়ার্ক ফোর্স স্টাডি’-এর প্রতিবেদন অনুযায়ী, বিশ্বজুড়ে প্রায় ৪৮ লাখ সাইবার নিরাপত্তা বিশেষজ্ঞের ঘাটতি রয়েছে। এ ঘাটতির ফলে বিশ্বের নানা দেশে গুরুত্বপূর্ণ অবকাঠামো সুরক্ষিত রাখা ও সংবেদনশীল তথ্যের নিরাপত্তা নিশ্চিত করা কঠিন হয়ে পড়ছে। বিশেষ করে, যেসব অঞ্চলে সম্পদ ও প্রযুক্তিগত সক্ষমতা সীমিত, সেখানে এ সংকট আরও প্রকট।

---

সাইবার নিরাপত্তা শিক্ষা ও প্রশিক্ষণকে সবার নাগালের মধ্যে আনার বিষয়ে দেশের নীতিনির্ধারকদের গুরুত্ব দিয়ে বিবেচনা করতে হবে। শুধু শহর নয়, গ্রামের তরুণদের জন্যও যেন এসব শিক্ষা ও প্রশিক্ষণ কর্মসূচি সহজলভ্য হয়, সেদিকেও নজর দিতে হবে।

বাংলাদেশের মতো উন্নয়নশীল দেশে দক্ষ জনবল তৈরির সুযোগ এখনো সীমিত। ফলে সাইবার নিরাপত্তা বিশেষজ্ঞের ঘাটতি এখানে আরও গভীর। কেবল হাতে গোনা কিছু শিক্ষাপ্রতিষ্ঠান এ বিষয়ে বিশেষায়িত কোর্স চালু করেছে, যেখানে আগ্রহী ও দূরদৃষ্টিসম্পন্ন তরুণেরা ভবিষ্যতের চাহিদা অনুযায়ী নিজেদের প্রস্তুত করার সুযোগ পাচ্ছে।

এস্তোনিয়া ও ফিনল্যান্ডের মতো দেশে সাইবার নিরাপত্তা শিক্ষার ইতিবাচক প্রভাব কতটা সুদূরপ্রসারী হতে পারে, তার উল্লেখযোগ্য উদাহরণ। ‘ই-স্তোনিয়া’ নামে পরিচিত এস্তোনিয়া তার নাগরিকদের অল্প বয়স থেকেই ডিজিটাল সাক্ষরতা ও সাইবার নিরাপত্তা বিষয়ে শিক্ষা প্রদান করে আসছে।

সাইবার নিরাপত্তাবিষয়ক শিক্ষা ও গবেষণায় পথিকৃৎ ফিনল্যান্ডও একইভাবে জাতীয় নিরাপত্তা ও শিক্ষাব্যবস্থার সঙ্গে সাইবার নিরাপত্তার বিষয়টি যুক্ত করেছে এবং সরকারি-বেসরকারি অংশীদারত্বের মাধ্যমে একটি শক্তিশালী সাইবার নিরাপত্তা ইকোসিস্টেম গড়ে তুলেছে। সিঙ্গাপুর, দক্ষিণ কোরিয়া ও সৌদি আরবও উল্লেখযোগ্যভাবে এই খাতে বিনিয়োগ করার মাধ্যমে দৃষ্টান্ত স্থাপন করেছে।

এই খাতে সাফল্য অর্জনে বাংলাদেশেরও প্রয়োজন বহুমুখী ও পরিকল্পিত উদ্যোগ গ্রহণ করা। প্রাথমিক পর্যায়ে থেকে বিশ্ববিদ্যালয় পর্যন্ত শিক্ষাক্রমে সাইবার নিরাপত্তা শিক্ষা অন্তর্ভুক্ত করা হতে পারে সে লক্ষ্য অর্জনে প্রথম পদক্ষেপ।

ডেটা সুরক্ষা, এথিক্যাল হ্যাকিং ও সাইবার হাইজিনের মতো বিষয়গুলো সম্পর্কে একদম তরুণ বয়সে ধারণা তৈরি হলে, তা শিক্ষার্থীদের মধ্যে এ খাত নিয়ে আগ্রহ তৈরি করবে। ভবিষ্যতে তারা এ খাতে নিজেদের ক্যারিয়ার গড়ে তোলার উৎসাহ পাবে।

সাইবার নিরাপত্তা শিক্ষা ও প্রশিক্ষণকে সবার নাগালের মধ্যে আনার বিষয়ে দেশের নীতিনির্ধারকদের গুরুত্ব দিয়ে বিবেচনা করতে হবে। শুধু শহর নয়, গ্রামের তরুণদের জন্যও যেন এসব শিক্ষা ও প্রশিক্ষণ কর্মসূচি সহজলভ্য হয়, সেদিকেও নজর দিতে হবে।

সাইবার সুরক্ষা খাতে ব্যবহারিক প্রশিক্ষণ অত্যন্ত গুরুত্বপূর্ণ। ‘সাইবার রেঞ্জ’-এর মতো সিমুলেটেড পরিবেশে শিক্ষার্থীরা অনুশীলনের সুযোগ পেলে, তারা বাস্তব পরিস্থিতিতে সাইবার ঝুঁকি মোকাবিলায় কৌশল কার্যকরভাবে রপ্ত করতে পারবে। পাশাপাশি বিশ্ববিদ্যালয় পর্যায়ে সাইবার নিরাপত্তা ও এআই গবেষণাকেন্দ্র স্থাপন করলে শিক্ষার্থীরা আন্তর্জাতিক মানের প্রকল্পে যুক্ত হতে পারবে এবং সমস্যা সমাধানের দক্ষতাও অর্জন করবে।

এ ছাড়া একটি শক্তিশালী সাইবার নিরাপত্তা কাঠামো এবং দক্ষ ও প্রশিক্ষিত বিশেষজ্ঞদের একটি বড় দল গড়ে তোলা বাংলাদেশের জন্য অত্যন্ত জরুরি। কারণ, এটি শুধু বিদেশি বিনিয়োগকারীদের আস্থা অর্জনের জন্য নয়, বরং দীর্ঘমেয়াদি অর্থনৈতিক প্রবৃদ্ধি নিশ্চিত করারও অন্যতম শর্ত।

আইটিইউ গ্লোবাল সাইবারসিকিউরিটি ইনডেক্স ২০২৪-এ বাংলাদেশকে ‘রোল মডেল’ হিসেবে স্বীকৃতি আমাদের সম্ভাবনা ও সক্ষমতা তুলে ধরার এক বড় সুযোগ এনে দিয়েছে। এ ক্ষেত্রে সুযোগের সঙ্গে প্রতিবন্ধকতাও আছে, কিন্তু এ প্রতিবন্ধকতাগুলো অতিক্রম করা অসম্ভব নয়। দৃঢ় পরিকল্পনা ও দক্ষ মানবসম্পদ গড়ে তুলতে পারলে বাংলাদেশ এই খাতে অনন্য অবস্থান তৈরি করতে পারে।

বিশ্বব্যাপী এআই-নির্ভর সমাধানের যুগে বাংলাদেশকেও নিজস্ব প্রতিভা বিকাশের কৌশল গ্রহণ করতে হবে। শিক্ষা, গবেষণা ও পারস্পরিক সহযোগিতার সমন্বয়ে একটি বাস্তবধর্মী কর্মপরিকল্পনা গড়ে তুলতে পারলে বাংলাদেশ সহজেই দক্ষিণ এশিয়ায় সাইবার নিরাপত্তা শিক্ষা ও সেবায় নেতৃত্বের অবস্থান নিতে পারবে। তবে এর জন্য প্রয়োজন দীর্ঘমেয়াদি কর্মপরিকল্পনা, যেখানে শিক্ষা ও উদ্ভাবন একে অপরের পরিপূরক হয়ে কাজ করবে; তখনই বাংলাদেশ এমন এক ভবিষ্যতের ভিত্তি স্থাপন করতে পারবে, যেখানে সাইবার নিরাপত্তা ও সাইবার উদ্ভাবন পাশাপাশি এগিয়ে যাওয়ার মাধ্যমে দেশের ডিজিটাল বিকাশকে আরও নিরাপদ ও টেকসই করে তুলবে।

- **হিউ গিল ইউনিভার্সাল কলেজ বাংলাদেশের (ইউসিবি) প্রেসিডেন্ট ও প্রভোস্ট**

