সাইবার সিকিউরিটি ও জাতীয় নিরাপত্তা

মোহাম্মদ জাবেদ মোর্শেদ চৌধুরী

একবিংশ শতাব্দীতে জাতীয় নিরাপত্তার সংজ্ঞাই পাল্টে গেছে। এখন জাতীয় নিরাপত্তা শুধু দেশের সীমান্তেই সীমাবদ্ধ নয়, বরং নিরাপত্তার সংজ্ঞা এখন ভার্চুয়াল দুনিয়া পর্যন্ত বিস্তৃত। তাই সাইবার অপরাধীরাও কোনো দেশের নিরাপত্তা ভাঙ্গার জন্য সাইবার অবকাঠামোকে টার্গেট করছে। অতিসম্প্রতি আমেরিকার নির্বাচনে তাদের দেশে রাশিয়ার হস্তক্ষেপ নিয়ে অনেক কথাবার্তা হচ্ছে। তবে সাইবার দস্যুতা আসলে কয়েক ধরনের হতে পারে।

০১. সুযোগসন্ধানী সাইবার দস্যুরা নিজেরা কোনো ভাইরাস বা আক্রমণ উদ্ভাবন করতে পারে না, কিন্তু অন্যের তৈরি করা আক্রমণ ব্যবহার করে। এদের মূল উদ্দেশ্য মাস্তানি বা বাজারে নাম কেনা। এরা সুযোগ পেলে বাহাদুরি করে, কিন্তু কোনো বড় ক্ষতি করার ক্ষমতা এদের নেই।

০২. আদর্শের জন্য সংগ্রামরত সাইবার দস্যু (হ্যাকটিভিস্ট), যারা কোনো আদর্শে উদ্বুদ্ধ হয়ে আক্রমণ করে।

০৩. অন্তর্ঘাতক সাইবার দস্যু, যারা কোনো কারণে ক্ষুব্ধ হয়ে নিজের দফতরকে আক্রমণ করে।

০৪. সংগঠিত অপরাধী সাইবার দস্যু (অর্গানাইজড ক্রিমিনাল হ্যাকার), অপরাধ যাদের পেশা এবং যারা এখন তথ্য-দস্যুতার মাধ্যমে টাকা বানাচ্ছে।

০৫. বিদেশি রাষ্ট্রীয় সাইবার দস্যু (নেশন স্টেট অ্যাক্টর), যখন একটি বিদেশি সরকার এ কাজে লিপ্ত হয়।

আমরা যখন দেখি একটি ওয়েবসাইট (বাংলাদেশ পুলিশ, র‍্যাব, সেনাবাহিনী ইত্যাদি) বদলে দিচ্ছে আক্রমণকারীরা, এরা সম্ভবত সুযোগ সন্ধানী বা আদর্শিক সাইবার দস্যু। আবার যখন আন্তর্জাতিক যুদ্ধাপরাধ ট্রাইব্যুনালের বিচারপতির কমপিউটার থেকে রায় বা তার স্কাইপ কথোপকথন রেকর্ড করে ফাঁস করা হচ্ছে, সেটা আদর্শিক সাইবার দস্যুতা। এরা ভুল আদর্শের জন্য বিচার বানচাল করতে চায়। আবার এতে ভিন্ন দেশের রাষ্ট্রীয় সাইবার দস্যুদের ভূমিকাও থাকতে পারে।

বাংলাদেশ ব্যাংক থেকে কোটি কোটি ডলার চুরি করেছে সংগঠিত অপরাধী সাইবার দস্যুরা। এরাই ক্রেডিট কার্ড চুরি করে। সাম্প্রতিক সময়ে বাংলাদেশে এটিএম থেকে চুরিও সংগঠিত অপরাধী সাইবার দস্যুদের কাজ। এবার দেখা যাক, সরকারি সাইবার দস্যুতার কিছু নমুনা।

০১. যুক্তরাষ্ট্র আর ইসরায়েল মিলে ইরানের আণবিক বোমা প্রকল্পের ক্ষতি করেছে স্টাক্সনেট নামে একটি ভাইরাস দিয়ে। চার বছর ধরে তারা তিল তিল করে ইরানের সবচেয়ে গোপন নেটওয়ার্কে ঢুকেছে, একটু একটু করে শিখেছে সেখানে কোথায় কী আছে, তারপর একটি বিশেষায়িত ভাইরাস দিয়ে গুরুত্বপূর্ণ কিছু যন্ত্র নষ্ট করে দিয়েছে।

০২. ইরানের সরকারি সাইবার বাহিনী আমেরিকান এয়ারফোর্সের ৬০ লাখ ডলার দামের একটি ড্রোনকে ভুল সঙ্কেত পাঠিয়ে ইরানে অবতরণ করিয়েছে। ড্রোনের দামের চেয়েও সেটা থেকে পাওয়া তথ্যের দাম ছিল বেশি এবং ইরানিরা সেই ড্রোনকে কপি করে এখন নিজেরাও ড্রোন বানিয়ে ফেলেছে।

০৩. যুক্তরাষ্ট্রের অফিস অব পার্সোনাল ম্যানেজমেন্টে (ওপিএম) চাইনিজ সাইবার দস্যুরা ১৮ মাস ধরে সব সরকারি কর্মচারীর তথ্য চুরি করেছে। এরকম আরও কয়েকশ' উদাহরণ আছে। এই লেখা সুযোগ সন্ধানী, আদর্শিক বা অন্তর্ঘাতক সাইবার দস্যুদের নিয়ে নয়। এমনকি সংগঠিত অপরাধী সাইবার দস্যুরাও এই লেখার মূল উদ্দেশ্য নয়। এই লেখার মূল উদ্দেশ্য রাষ্ট্রীয় সাইবার দস্যুতা এবং বাংলাদেশের সাইবার অবকাঠামোর ঝুঁকি আর নিরাপত্তা নিয়ে।

বাংলাদেশের মতো ছোট দেশের রাষ্ট্রীয় সাইবার দস্যুদের নিয়ে ভয় পাওয়ার কিছু আছে কী? হয়তো অবাক হবেন, কিন্তু বাংলাদেশে বিদেশী রাষ্ট্রীয় সাইবার দস্যুরা অনেক আগেই হানা দিয়েছে। ২০০৯ সালে ঘোস্টনেট নামে একটি ভাইরাস পাওয়া গেছে বাংলাদেশ পররাষ্ট্র মন্ত্রণালয়ের কমপিউটারে। এ ছাড়া ২০১২ ও ২০১৩ সালে পররাষ্ট্র মন্ত্রণালয়ের ওয়েবসাইট হ্যাক করেছিল কিছু আদর্শিক সাইবার দস্যু।

আমেরিকা, রাশিয়া, চীন ও বড় সব দেশের সামরিক বাহিনীতে এখন সাইবারযুদ্ধের জন্য আলাদা বাহিনী আছে। কারণটা খুব সহজ। এই সাইবার মাধ্যমে অনেক কম খরচে, গোপনে অনেক বেশি ক্ষতি করা যায় শত্রুপক্ষের। একটি উদাহরণ দেয়া যাক, একটি এফ-১৬ যুদ্ধবিমানের দাম দুই হাজার কোটি টাকা। সেটা দিয়ে দ্রুত আক্রমণ করা যায় ঠিকই, কিন্তু যদি শত্রু সেটাকে ধ্বংস করে দিতে পারে, তাহলে এত দামী যুদ্ধবিমান আর একজন পাইলটের প্রাণ, যেটার দাম পরিমাপ করা সম্ভব নয়, তা নিঃশেষ হয়ে যাবে। ইরানের আণবিক বোমার গবেষণাগার মাটির এক হাজার ফুট নিচে। বিমান থেকে ফেলা বোমা দিয়ে সেটা ধ্বংস করা সম্ভব নয় এবং বোমা মারলে সরাসরি যুদ্ধ বেধে যাবে। কিন্তু মাত্র কয়েক মিলিয়ন ডলার খরচ করে বানানো স্টাক্সনেট ভাইরাস দিয়ে যুক্তরাষ্ট্র ইউরেনিয়াম আলাদা করার সেন্ট্রিফিউজ যন্ত্র ভেঙে দিয়ে ইরানের আণবিক গবেষণা কয়েক বছর পিছিয়ে দিয়েছিল।

কীভাবে স্টাক্সনেট এই গোপন গবেষণাগারে ঢুকল, জানেন? একজন মার্কিন চর একটা পার্কিং লটে কিছু ইউএসবি বা পেনড্রাইভ ফেলে এসেছিল, যাতে ছিল একটা সম্পূর্ণ নতুন ভাইরাস, যা কোনো অ্যান্টিভাইরাস আটকাতে পারে না। গবেষণাগারের একজন কর্মচারী একটা পেনড্রাইভ তুলে নিয়ে নিজের অফিসের কমপিউটারে লাগান এবং তারপর বাকিটুকু ইতিহাস।

বাংলাদেশের পরিপ্রেক্ষিতে একটি বিদ্যুৎকেন্দ্র বাংলাদেশের একটি গুরুত্বপূর্ণ স্থাপনা, যা নষ্ট করে দিলে বাংলাদেশের জানমালের বিশাল ক্ষতি হতে পারে। কিছুদিন আগেই আমরা দেখেছি গ্রিড বিপর্যয় কত ক্ষতিকর হতে পারে। ভাইরাস পাঠিয়ে জেনারেটর ধ্বংস করেছেন যুক্তরাষ্ট্রের গবেষকেরা। সুতরাং এটি শুধু সিনেমার প্লট নয়, এটা বাস্তব। গ্যাস বা বিদ্যুৎ উৎপাদন, সঞ্চালন এগুলো নিয়ন্ত্রণ এবং তথ্য জোগাড় করা হয় স্ক্যাডা নামে একটি প্রণালী দিয়ে। ওপরে বর্ণিত স্টাক্সনেট স্ক্যাডা যন্ত্রপাতিকে আক্রমণ করেছিল। যেসব ভাইরাস দিয়ে এরকম অবকাঠামো সহজে ধ্বংস করে দেয়া যায়, সেগুলো যেকোনো মারণাস্ত্রের চেয়েও ভয়াবহ।

সাইবার দস্যুরা আপনার ফোন থেকে আপনার অবস্থান জানতে পারে। কিছু সফটওয়্যার দিয়ে সাইবার দস্যুরা ফোনের কথা শুনতে পারে, ক্ষুদে বার্তা চুরি করতে পারে। রাষ্ট্রীয় গুরুত্বপূর্ণ ব্যক্তিদের অবস্থান যদি শত্রুরা জানতে পারে, তাদের সব কথা শুনতে পারে, তা বাংলাদেশের জন্য ভীষণ বিপজ্জনক। তেলের কূপের কন্ট্রাক্ট সরকার কত দামে ছেড়ে দেবে অথবা আগামী বাজেটে কোন পণ্যের ওপর নতুন কর আসছে, সেটা জেনে দেশের অর্থনৈতিক ক্ষতি করা যায়। একজন বিচারপতি একটি গুরুত্বপূর্ণ মামলার রায় সম্পর্কে কী ভাবছেন, সেটা জেনে নিয়ে দেশের ভাবমূর্তির ক্ষতি করা সম্ভব।

আমরা পৃথিবী থেকে বিচ্ছিন্ন নই। বাংলাদেশ ব্যাংকের ওপর সাম্প্রতিক আক্রমণ, পররাষ্ট্র মন্ত্রণালয়ে বিদেশী ভাইরাস, বিচারপতির রায়ের খসড়া চুরি– এগুলো প্রমাণ করে যে দেশী-বিদেশী শত্রুরা বাংলাদেশের ক্ষতি করতে প্রস্তুত। এই শত্রুদের বিরুদ্ধে প্রতিরক্ষা গড়ে তোলাই এখন সবচেয়ে জরুরি বিষয় হিসেবে বিবেচনা করা প্রয়োজন।

একটি পরিপূর্ণ প্রতিরক্ষা পরিকল্পনা এই লেখার পরিসরের বাইরে, তবে একটি কাজ খুব সহজেই করা যেতে পারে, যা থেকে দীর্ঘমেয়াদী সুফল আসবে। বাংলাদেশ ব্যাংকের ওপর এই আক্রমণের পর দেশে প্রশিক্ষিত, অভিজ্ঞ তথ্য নিরাপত্তা বিশেষজ্ঞদের অভাব খুব প্রকটভাবে চোখে পড়েছে। বিশ্ববিদ্যালয়গুলোতে সাইবার নিরাপত্তার ওপর শিক্ষাক্রম শুরু করতে হবে, যাতে আমাদের দেশেই দক্ষ সাইবার নিরাপত্তা জনশক্তি গড়ে ওঠে। তাতে আমাদের সাইবার নিরাপত্তা ও প্রতিরক্ষা আরও মজবুত হবে কজ

ফিডব্যাক : jabedmorshed@yahoo.com