بسم اللہ الرحمٰن الرحیم

مصنوعی ذہانت (آرٹیفیشل انٹیلیجنس) اور خود مختار سائبر سکیورٹی!

(ترجمہ)

https://www.al-waie.org/archives/article/20482

الوعي میگزین – شمارہ نمبر 482

اکتالیسواں سال

ربیع الاول 1448ھ

بمطابق اگست 2026ء

تحریر : عبد الحلیم الحوراني

میں یہ سطور اس ادراک کے ساتھ لکھ رہا ہوں کہ جو کچھ آگے بیان کیا جائے گا، اس کا بہت سا حصہ جلد ہی مانوس محسوس ہونے لگے گا؛ اس میدان میں تبدیلی کی رفتار ہماری اسے دستاویزی شکل دینے کی صلاحیت سے بھی آگے نکل چکی ہے۔ مسئلہ اب محض تحقیق کا موضوع نہیں رہا؛ **مصنوعی ذہانت (آرٹیفیشل انٹیلیجنس)** سائبر جنگ کے میدان میں عملی طور پر داخل ہو چکی ہے اور ہماری روزمرہ زندگی کی تفصیلات تک میں سرایت کر چکی ہے۔ آج کے دور میں جو ریاست اپنے دفاع کے مستحکم ہونے میں پیچھے رہ گئی، تو اسے صرف ایک یا دو شعبۂ نظام نہیں بلکہ اپنی مکمل گنجائشِ عمل سے محروم ہونے کا خطرہ ہے—یعنی یہی وہ وقت ہے جب اس ریاست کو فیصلہ سازی کے لئے اپنی خودمختار طاقت استعمال کرنے کی سب سے زیادہ ضرورت ہوتی ہے۔ اگرچہ تیاری پر بھاری اخراجات آتے ہیں، لیکن جب کڑا وقت آ گیا تو تیاری نہ کرنے کا پچھتاوا کہیں زیادہ مہنگا ثابت ہوگا۔

آخر کیسے مصنوعی ذہانت نے کھیل کے اصول ہی بدل دئیے ہیں؟

مصنوعی ذہانت کی مختلف اقسام کے بارے میں ایک عام غلط فہمی پائی جاتی ہے، جو اس ٹیکنالوجی سے وابستہ خطرات کے بارے میں ہماری سمجھ کو متاثر کرتی ہے۔ عام لوگوں کے سمجھنے کے لئے اسے آسان بنانے کی خاطر ہم ان اقسام میں یوں فرق کر سکتے ہیں:

- **امتیازی مصنوعی ذہانت (Discriminative AI)** : یہ قسم سب سے پرانی اور سب سے زیادہ رائج ہے؛ اس کا کام اشیاء کو ترتیب دینا اور ان کی درجہ بندی کرنا ہے۔ یہ تقریباً ان ای میل فلٹرز کی طرح کام کرتی ہے جو خودکار طور پر

غیرضروری (spam) میسجز کی پہچان کر لیتے ہیں اور پھر ان کی درجہ بندی کرتے ہیں۔

- **تخلیقی مصنوعی ذہانت (Generative AI) :** یہ وہ قسم ہے جو جدید ماڈلز، جیسےChatGPT ، میں دیکھی جاتی ہے؛ **AI** کی یہ قسم تخلیقی صلاحیت رکھتی ہے اور ان معلومات کی بنیاد پر بالکل نیا مواد تیار کر سکتی ہے جن پر اسے ہدایات دی گئی ہوں۔

ان تخلیقی ماڈلز کی آمد سے پہلے سائبر حملوں کی چھان بین کے لئے منظم ٹیموں اور بڑے بجٹ کی ضرورت ہوتی تھی، اور اسی لئے یہ جارحانہ صلاحیتیں بڑی طاقتوں اور چند مخصوص گروہوں کے ہاتھوں تک ہی محدود تھیں۔ لیکن آج مصنوعی ذہانت نے جارحانہ کارروائیوں کی لاگت میں کافی نمایاں حد تک کمی کر دی ہے، جس سے متوسط درجے کی مہارت رکھنے والے چھوٹے گروہوں یا افراد کے لئے بھی نہایت کم لاگت پر سنگین نقصان پہنچانا ممکن ہو گیا ہے۔ جارحانہ کارروائیوں میں اہم تبدیلیاں یہ ہیں :

- **سمارٹ جاسوسی(Smart Reconnaissance) :** وہ کام جن کے لئے پہلے معلومات جمع کرنے اور ہدف کا کھوج اور باریکیاں تلاش کرنے میں انسانی محنت کے کئی ہفتے درکار ہوتے تھے، اب وہ کام ڈیجیٹل ایجنٹس محض چند گھنٹوں میں انجام دے رہے ہیں—اور موجودہ دفاعی صلاحیتوں سے بھی آگے نکل رہے ہیں۔
- **خودکار کمزوریوں کی تیاری (Automated Vulnerability Generation):** مصنوعی ذہانت کے آلات سافٹ ویئر کو کمزوریوں کے لئے اسکین کرتے ہیں اور ریکارڈ وقت میں انہیں حقیقی ایکسپلائٹ کوڈ میں تبدیل کر دیتے ہیں، جس سے اس ٹارگٹ کی اپنے سسٹمز کو درست کرنے کی صلاحیت پیچھے رہ جاتی ہے۔
- **سمارٹ سپئیر فشنگ (Smart Spear-Phishing) :** ناکارہ اور ناقص فشنگ ای میلز کا دور ختم ہو چکا ہے؛ مصنوعی ذہانت اپنے شکار کے ڈیجیٹل فٹ پرنٹس اور کمیونیکیشن انداز کا تجزیہ کر کے خود سے ایسے ذاتی نوعیت کے پیغامات تیار کر لیتی ہے جن کا سراغ لگانا تجربہ کار ماہرین کے لئے بھی کافی مشکل ہوتا ہے۔
- **ڈیپ فیکس (Deepfakes) :** محض ظاہری استدلال سے آگے بڑھتے ہوئے، اب ایک مختصر آڈیو نمونہ ہی کسی آواز کو انتہائی درستگی کے ساتھ نقل کرنے کے لئے کافی ہے، جس سے جعلی آڈیو یا ویڈیو گفتگو تیار کی جا سکتی ہے تاکہ اپنے شکار کو دھوکہ دیا جائے اور انہیں بڑے پیمانے پر مالی رقوم منتقل کرنے کی منظوری دینے پر آمادہ کیا جائے۔
- **پولی مورفک مالویئر(Polymorphic Malware) :** ایسا نقصان دہ سافٹ ویئر ہے جو ہر ٹرانسمشن کے ساتھ اپنی شکل اور کوڈ تبدیل کرتا رہتا ہے، نقصان دہ

وائرس کا پتہ لگانے والے روایتی سسٹمز (detection systems) کو الجھا دیتا ہے اور پتہ چلنے کے بغیر ہی وائرس کو اس سسٹم کے اندر موجود رہنے دیتا ہے۔

مصنوعی ذہانت کے ''دماغ'' پر حملے :

بہرحال ایک بنیادی تبدیلی واقع ہو چکی ہے: اب ہدف صرف نیٹ ورک کے نظام نہیں بلکہ خود مصنوعی ذہانت کا ''دماغ'' بھی ہے۔ یہ حملے بنیادی طور پر تین شکلیں رکھتے ہیں:

1- مصنوعی ذہانت کو جان بوجھ کر غلط معلومات فراہم کرنا (Data Poisoning) :
حملہ آور ہدایات دینے کے مرحلے کے دوران غلط معلومات داخل کر دیتے ہیں، جس سے سسٹم پتہ لگے بغیر ہی غلط منطق اختیار کر لیتا ہے۔ مثال کے طور پر، تعمیراتی معاہدوں کے آڈٹ کے ایک سسٹم کو خفیہ طور پر اس طرح ہدایات دی گئیں کہ وہ مخصوص معاہدوں میں تاخیر ہونے پر پڑنے والے جرمانوں کو نظر انداز کر دے۔

2-چالاکی سے تیار کردہ جعلی معلومات کے ذریعے سسٹم کو گمراہ کرنا (Deception Attacks): ٹریننگ مکمل ہونے کے بعد حملہ آور ماڈل کو دھوکہ دینے کے لئے باریک بینی سے تبدیل کی گئی ان پٹس داخل کرتا ہے—مثلاً وائرس فائل میں ایسی معمولی تبدیلی جو سکیورٹی سسٹم کو اسے ایک عام ٹیکسٹ فائل سمجھنے پر مجبور کر دے، یا کسی تصویر میں ایسی ناقابلِ محسوس تبدیلی جو چہرے کی شناخت کرنے والے سسٹم کو الجھا دے۔

3- سسٹم کے راز اور اندرونی ڈیٹا کو چوری کرنا (Model Extraction) :
حساس ڈیٹا حاصل کر لینا یا خود الگورتھم کا چوری کر لینا؛ اگر کسی سسٹم کو کسی کمپنی کے تجارتی رازوں پر ہدایات دی گئی ہوں تو حملہ آور چالاک سوالات کے ذریعے اس سسٹم کو وہ خفیہ معلومات ظاہر کرنے پر مجبور کر سکتا ہے۔

بحران کی زد میں اہم شعبے: تباہی کی نوعیت اور صورت کیا ہو سکتی ہے ؟

تمام شعبے یکساں قدر نہیں رکھتے؛ قومی اہمیت کے بنیادی ڈھانچے کا تحفظ اولین ترجیح ہوتا ہے۔ ذیل میں چار حقیقت پسندانہ منظرنامے دئیے گئے ہیں جو یہ واضح کرتے ہیں کہ مصنوعی ذہانت خطرے کی نوعیت کو کیسے تبدیل کر سکتی ہے:

پہلا منظرنامہ: بجلی کے گرڈ اور توانائی کے شعبے کا انہدام

مصنوعی ذہانت کے ذریعے کیا جانے والا مربوط حملہ صنعتی کنٹرول سسٹمز کی کمزوریوں سے فائدہ اٹھاتے ہوئے بیک وقت متعدد بجلی کے سب اسٹیشنوں کو نشانہ بناتا ہے۔ چند منٹوں کے اندر ہی ایک کے بعد دوسری خرابیاں رونما ہونا شروع ہو جاتی ہیں؛ پھر چند ہی گھنٹوں میں ملک بجلی سے محروم ہو جاتا ہے اور ہسپتالوں اور ڈیٹا سینٹرز

میں بیک اپ بیٹریاں بھی ختم ہو جاتی ہیں۔ یہ تباہی صرف ملک کے اندھیرے میں ڈوب جانے میں نہیں بلکہ اس کے فوری بعد پیدا ہونے والی مکمل مفلوج پن کی صورتحال میں ہے، جب مواصلات، بینکاری اور الیکٹرانک ادائیگی کے سسٹمز بھی ناکام ہو جاتے ہیں۔ مصنوعی ذہانت سے تقویت یافتہ اس منظرنامے میں مسئلہ ''پوائنٹ بمقابلہ پوائنٹ'' کا نہیں—جیسا کہ 2015ء میں یوکرین میں دیکھا گیا—بلکہ ''الگورتھم بمقابلہ الگورتھم'' کا ہے، جہاں کاری وار بیک وقت متعدد حملوں کو مربوط کرتا ہے اور فوراً ہی دفاعی اقدامات کے مطابق خود کو ڈھال رہا ہوتا ہے۔

دوسرا منظرنامہ: بینکاری اور مالیاتی نظام کا مفلوج ہونا

ایک کثیر سطحی حملہ ایک اعلیٰ سطحی مالیاتی عہدیدار کی ڈیپ فیک کال سے شروع ہوتا ہے، جس کے ساتھ ہی بینکاری کے باضابطہ رقوم منتقلی سسٹم پر رینسم ویئر حملہ کر دیا جاتا ہے۔ چند گھنٹوں میں فوری ادائیگیاں رک جاتی ہیں؛ ایک ہی دن کے اندر لوگ بڑے پیمانے پر نقد رقم نکلوانے کے لئے اے ٹی ایمز پر قطاریں لگا دیتے ہیں، جبکہ خودکار اکاؤنٹس افواہیں پھیلاتے ہیں جو قومی کرنسی پر اعتماد کو کمزور کرتی ہیں۔ یہ منظرنامہ 2022ء میں کوسٹا ریکا میں پیش آنے والے واقعے سے مماثل ہے، جہاں ایک رینسم ویئر حملے نے ریاستی اداروں کو مفلوج کر دیا تھا اور ہنگامی حالت کا اعلان کرنے پر مجبور کر دیا تھا؛ تاہم مصنوعی ذہانت کی آمد کے ساتھ صورتحال عملی مفلوج پن سے بڑھ کر مالیاتی خودمختاری کے مکمل بحران میں تبدیل ہو سکتی ہے۔

تیسرا منظرنامہ: سماجی اعتماد اور انفارمیشن ماحول کا زوال

یہ سب سے خطرناک منظرنامہ ہے، کیونکہ اس کے لئے کسی ٹیکنیکل سسٹم کو توڑنے کی ضرورت نہیں بلکہ انٹرنیٹ کی کھلی نوعیت سے فائدہ اٹھانا ہی کافی ہے۔ مصنوعی ذہانت ہزاروں مربوط خودکار اکاؤنٹس تیار کرتی ہے جو سرکاری اہلکاروں کی اعلیٰ معیار کی ڈیپ فیک ویڈیوز اور معروف میڈیا اداروں کی نقل کرتے ہوئے مضامین پھیلانا شروع کر دیتے ہیں۔ اس کا مقصد ہر شخص کو قائل کرنا نہیں بلکہ بڑے پیمانے پر شک پیدا کرنا ہے، جس سے شہری حقیقی اور جعلی کے درمیان فرق کرنے سے قاصر ہو جائیں۔ اس سے ریاست کی بحرانوں کو سنبھالنے کی صلاحیت مفلوج ہو جاتی ہے، کیونکہ ہر سرکاری بیان شک و شبہ سے دیکھا جاتا ہے۔ محققین اسے ''جھوٹے کو فائدہ (liar's dividend) کہتے ہیں، اور اس کے رونما ہونے کا امکان سب سے زیادہ ہوتا ہے۔

چوتھا منظرنامہ: ہتھیاروں اور ڈیفنس سسٹم کا ہائی جیک کر لینا

ڈرونز اور خودکار سسٹمز کے پھیلاؤ کے ساتھ کنٹرول سسٹمز کو بھی نشانہ بنانے کا خطرہ پیدا ہو گیا ہے، جس کے ذریعے ڈرونز کے بیڑے کو ناکارہ بنایا جا سکتا ہے یا انہیں ان کے اپنے مالک کے خلاف استعمال کیا جا سکتا ہے۔ اس کے لئے سافٹ ویئر کی سپلائی چین کو متاثر کرنا یا ٹارگٹ کی شناخت کے ڈیٹا کو مسخ کرنا درکار ہوتا ہے۔ متعدد

محاذوں پر نیویگیشن سسٹم میں مداخلت کے ایسے واقعات دیکھے گئے ہیں جن کے نتیجے میں ڈرونز واپس مڑ کر اپنی ہی افواج کی طرف آ گئے؛ مزید برآں، جیسے جیسے مصنوعی ذہانت سے کئے جانے والے حملے ترقی کر رہے ہیں، یہ بھی ممکن ہو جاتا ہے کہ ایک دوست ریڈار کسی دوست اثاثے کوہی اپنا دشمن سمجھ لے، یا اسی طرح اس کے برعکس بھی ممکن ہے۔

کیا کوئی ریاست واقعی منہدم بھی ہو سکتی ہے؟

اس سوال کا جواب زوال کی نوعیت پر منحصر ہے :

- **اچانک اور مکمل انہدام :** اس کا امکان کم ہے؛ جدید ریاستوں کے پاس متعدد متبادل اور اضافی سسٹمز موجود ہوتے ہیں جو تمام شعبوں کو بیک وقت ناکام ہونے سے روکتے ہیں۔ عسکری افواج ایک علیحٰدہ نیٹ ورکس پر کام کر رہی ہوتی ہیں، اور بنیادی ڈھانچے کے اہم سسٹمز میں اکثر مینوئل کنٹرول کی صلاحیت موجود ہوتی ہے۔
- **بتدریج، کثیر مرحلہ جاتی مفلوج پن :** اس کا امکان کہیں زیادہ ہے؛ تیزی سے یکے بعد دیگرے تین یا چار شعبوں کو نشانہ بنانے والا مربوط حملہ، اور ساتھ ہی غلط معلومات پھیلانے کی مہم ، تو ایسا حملہ ریاست کو مؤثر کنٹرول کھونے کی حد تک پہنچا سکتا ہے۔ ان دونوں میں فرق، ایک دھماکے کی آگ اور ایک آہستہ آہستہ پھیلنے والی تباہ کن آگ کے فرق جیسا ہے: ایک ریاست چند ماہ میں کسی قدرتی زلزلے سے تو بحال ہو سکتی ہے، جبکہ ایک ''سائبر زلزلہ'' جو اعتماد کو ہی چکنا چور کر دے، اسے ٹھیک ہونے میں برسوں لگ جاتے ہیں۔

تین گنا فائر وال: ایک ریاست اپنی آزادی اور فیصلہ سازی کی خودمختاری کو کیسے محفوظ رکھ سکتی ہے؟

مؤثر دفاع منتشر اقدامات سے نہیں کیا جاتا بلکہ ایک مربوط نظام سے تشکیل پاتا ہے، جس کے تین بنیادی ستون ہوتے ہیں:

1- امورِ حکمرانی اور قوانین (Regulation)

ایک سائبر سکیورٹی اور مصنوعی ذہانت کی اتھارٹی قائم کرنا، جس کی منیجمنٹ آزاد و خودمختار ہو، جس کے ماتحت سائبر کمانڈ ہو، اور جو براہِ راست ریاست کی اعلیٰ ترین قیادت کو رپورٹ کرے۔ اس کا اختیار حساس شعبوں کے لئے پابند ضوابط اور ہدایات نافذ کرنا اور کم از کم معیارات اور کنٹرول کے اقدامات مقرر کرنا ہو۔

2- ٹیکنیکل خودمختاری کی صلاحیتیں(The Machine)

خودمختاری کا تقاضا ہے کہ اہم مراکز پر مکمل کنٹرول حاصل کیا جائے؛ اس مقصد کے لئے حساس حکومتی ڈیٹا کو محفوظ کرنے اور پروسیس کرنے کے لئے آزاد کلاؤڈ انفراسٹرکچر قائم کیا جائے، خصوصی کمپیوٹنگ مراکز بنائے جائیں اور مقامی طور پر آزاد ڈیٹا پر تربیت یافتہ بنیادی مصنوعی ذہانت کے ماڈلز تیار کیے جائیں۔

3- افرادی قوت (The Human)

افرادی قوت کے بغیر ٹیکنالوجی ایک خالی خول ہوتی ہے۔ ایک کامیاب منصوبہ انسانوں کو اولین ترجیح دیتا ہے، اعلیٰ مہارت رکھنے والی خصوصی ٹیمیں اور تحقیقی مراکز تیار کرتا ہے جو مختلف شعبوں—بشمول انٹیلی جنس، انجینئرنگ، نفسیات، معاشیات اور سیاسیات—میں ماہرین کی ایک فوج تیار کرنے کے قابل ہوں، تاکہ دفاع اور حملے کا ایک مربوط ماحولیاتی سسٹم تشکیل دیا جا سکے۔

دفاعی نظاموں کی فوج اور ریاستی پروٹوکول

''مصنوعی ذہانت کی دفاعی فوج'' کا تصور اس حقیقت سے پیدا ہوتا ہے کہ تیز رفتار مشین کا مقابلہ صرف سست انسانی ذہنوں سے نہیں کیا جا سکتا؛ حملے بجلی کی رفتار سے ہوتے ہیں اور اسکرینوں کے پیچھے بیٹھا عملہ انہیں روک نہیں سکتا۔ اس کے بجائے ہمیں ایسے دفاعی ''خودکار سسٹم'' درکار ہیں جو ایک سیکنڈ کے بھی اعشاریہ حصے میں جواب دینے کی صلاحیت رکھتے ہوں۔ اس نظام کے تین اجزاء ہیں :

اول: ذہین ڈیجیٹل سسٹم

- **انٹیلیجنٹ آپریشنز سینٹر :** ایک نگرانی کا مرکز جو ہزاروں چھوٹے سے چھوٹے الرٹس کو بھی فلٹر کرتا ہے اور معمولی مسائل کو خودکار طور پر حل کر لیتا ہے، جبکہ بڑے اور حساس فیصلے انسانوں میں منتظمین کو بھیجتا ہے۔
- **فعال شکاری(Proactive Hunter) :** حملہ شروع ہونے سے پہلے ہی سسٹم میں موجود کسی بھی خفیہ درانداز کے آثار تلاش کرنے کے لئے ڈیجیٹل ایجنٹس تعینات کرنا؛ روک تھام کرنا ٹھیک کرنے سے کم مہنگا ہوتا ہے۔
- **اخلاقی جارحانہ جانچ کی ٹیمیں :** ایسے سافٹ ویئر اور ہیکرز جن کی یہ ذمہ داری ہو کہ وہ ریاستی نظاموں پر مسلسل حملے کریں تا کہ کمزوریوں کی پہچان ہو سکے اور انہیں دور کریں، اس سے پہلے کہ دشمن ان سے فائدہ اٹھا سکیں۔

دوم: ڈیجیٹل خودمختاری اور مواد کا تحفظ

- **ڈیجیٹل سیلنگ (مہر لگا دینا) :** سرکاری ڈیٹا پر ایک نظر نہ آنے والا ڈیجیٹل تصدیقی نشان لگانا تاکہ معاشرے کو افواہوں اور انفارمیشن ابہام سے محفوظ رکھا

جا سکے؛ ایسی کوئی بھی اطلاع جس پر یہ مہر موجود نہ ہو، جعلی تصور کی جائے۔

- **ٹیکنیکل خودمختاری :** ایسی مقامی مصنوعی ذہانت تیار کرنا جو ہماری ثقافت کو سمجھتی ہو اور ریاستی ڈیٹا کی رازداری کا تحفظ کرتی ہو، بجائے اس کے کہ بیرونی کمپنیوں پر انحصار کیا جائے جو ڈیٹا افشا کر سکتی ہیں۔

سوم: ریاست اور فرد کی حکمت عملی

- **جامع سائبر مشقیں :** صرف ٹیکنیکل ٹیموں کو ہی نہیں بلکہ پوری حکومت کے ردعمل کی جانچ کرنا، تاکہ خامیوں کی نشاندہی ہو اور لیڈران کو ڈیجیٹل ہنگامی حالات سنبھالنے کی تربیت دی جا سکے۔
- **اہم کاروباری تسلسل کے منصوبے :** ہر شعبے کے لئے ٹیسٹ شدہ ایک سالانہ منصوبہ، جس میں مختلف قسم کے ہنگامی منظرنامے شامل ہوں جیسا کہ مکمل نظام کی ناکامی، مینوئل آپریشنز کی طرف منتقلی اور متبادل کمیونیکیشن ذرائع کے استعمال۔
- **ملٹی-سورس ٹیکنیکل ریزروز :** کسی ایک ٹیکنالوجی فراہم کرنے والی کمپنی یا کسی ایک ملک پر انحصار سے گریز کرنا، کیونکہ ایسا انحصار ایک خطرناک اسٹریٹجک کمزوری پیدا کر دیتا ہے۔
- **پہلے سے قائم لوکل ردعمل کا پروٹوکول:** فیصلہ سازی کی واضح درجہ بندی اور مخصوص اتھارٹیز متعین کرنا تاکہ پہلے سے مقرر کردہ سائبر ہنگامی قوانین کو فعال کیا جا سکے؛ کیونکہ ایک بحران کی صورتحال میں پروٹوکول تیار کرنے کا وقت نہیں ہوتا۔
- **سماجی سکیورٹی کلچر:** مسلسل آگاہی مہمات، عملے کی تربیت اور تعلیمی نصاب میں بنیادی سکیورٹی اصولوں کو شامل کرنا، تاکہ شہریوں کی آگاہی دفاع کی پہلی صف بن جائے۔

پوسٹ کوانٹم کرپٹوگرافی

ایک ایسا خطرہ منڈلا رہا ہے جو روایتی معنوں میں ''سائبر'' نہیں: انتہائی طاقتور کوانٹم کمپیوٹرز۔ جب یہ مشینیں مکمل طور پر میچور ہو جائیں گی تو یہ ان بیشتر انکرپشن الگورتھمز کو توڑنے کے قابل ہوں گی جو اس وقت حکومتی ڈیٹا کے تحفظ کے لئے استعمال ہوتے ہیں۔ خوفناک خطرہ صرف مستقبل میں نہیں بلکہ ابھی سے جاری ہے، جسے ایک مخالفانہ حکمت عملی ''اب جمع کرو، بعد میں ڈیکرپٹ کرو (Harvest Now, Decrypt Later)'' کہا جاتا ہے۔ مخالفین آج انکرپٹ شدہ ڈیٹا کو، جو زیرِ سمندر کیبلز اور

سیٹلائٹس کے ذریعے منتقل ہوتا ہے، حاصل کر کے محفوظ کر رہے ہیں اور اس مستقبل کے لمحے کے منتظر ہیں جب انتہائی طاقتور کمپیوٹنگ نظاموں کی آمد کے ساتھ انکرپشن توڑ دی جائے گی۔ لہٰذا فوری منصوبے کی ضرورت ہے، جس میں درج ذیل اقدامات شامل ہوں :

1- اہم حکومتی نظاموں میں استعمال ہونے والے الگورتھمز کی جامع فہرست تیار کرنا۔

2- ڈیٹا کو اس کی ''انڈیپنڈنٹ لائف'' کے مطابق درجہ بند کرنا، یعنی وہ مدت جس کے دوران ڈیٹا حساس رہتا ہے اور تحفظ کا متقاضی ہوتا ہے۔

3- منظور شدہ کوانٹم مزاحم اسٹینڈرڈز کی طرف بتدریج منتقلی شروع کرنا اور اس بات کو یقینی بنانا کہ ہر نئی ترقی پہلے دن ہی سے کرپٹوگرافک مشکلات سے سنبھل جانے کی صلاحیت رکھتی ہو۔

نتیجہ اور اسٹریٹجک تجویز

آج حقیقی خطرہ ریاست کا اچانک انہدام نہیں بلکہ اس کی اسٹریٹجک نقل وحمل کی قابلیت کی گنجائش کا خاتمہ اور ایک نازک مرحلے میں اس کے اداروں پر اعتماد کا زوال ہے۔ ایک ایسی ریاست جو ایسے ماحول میں بھی آگے بڑھتی رہے اور ایک ایسی ریاست جو لڑکھڑا جائے ، ان دونوں ریاستوں کے درمیان فرق ان کے وسائل کی مقدار میں نہیں بلکہ ان کی انتظامی سوچ میں ہوتا ہے: جو ریاست سائبر سکیورٹی اور مصنوعی ذہانت کو محض ٹیکنیکل مسائل سمجھتی ہے جنہیں وزارتِ مواصلات یا آئی ٹی کا محکمہ سنبھالے گا، تو ایسی ریاست خود کو کئی نسلیں پیچھے پائے گی؛ جبکہ جو ریاست انہیں خودمختاری کے معاملات سمجھ کر اعلیٰ ترین سیاسی سطح پر منظم کرے گی، وہ خود کو ہر قسم کی تیاری اور اثر و رسوخ کے لئے تیار کرے گی۔ مواقع کی کھڑکی ابھی کھلی ہے، لیکن اس میدان میں صرف ایک سال کی تاخیر بھی دوسرے شعبوں میں ایک دہائی پیچھے رہ جانے کے مترادف ہے، کیونکہ ٹیکنیکل ترقی اور پیش رفت کی رفتار حیران کن حد تک تیز ہے۔