The Trojan Horse: Ancient myths to Modern Digital World—Strategy and Deceit

ٹروجن ہارس: قدیم اساطیر سے جدید ڈیجیٹل دنیا تک — فریب اور حکمتِ عملی کا ارتقا

Nayab Ghafoor *[1]
Ph.D. Scholar Urdu, Urdu Department, NUML, Islamabad
Dr. Mehmood Ul Hassan*[2]
Assistant Professor, Department of Urdu ,NUML,Islamabad.

نایاب غفور☆[1]
پی ایچ ڈی سکالر، شعبہ اردو، نیشنل یونیورسٹی آف ماڈرن لینگویجز، اسلام آباد
ڈاکٹر محمود الحسن☆[2]
اسسٹنٹ پروفیسر، شعبہ اردو، نیشنل یونیورسٹی آف ماڈرن لینگویجز، اسلام آباد

Correspondance: nayabghafoor@gmail.com

eISSN:**3005-3757**
pISSN: **3005-3765**

Received: 24-01-2026
Accepted:22-03-2026
Online:31-03-2026

ABSTRACT: The Trojan Horse is one of the most enduring symbols of deception and strategic intelligence in human history. Originating from Greek mythology, it represents a powerful narrative of how appearances can conceal dangerous intentions. This article explores the transformation of the Trojan Horse from an ancient war strategy into a modern metaphor widely used in cyber security, politics, and social systems. The study examines how deception, as a fundamental human strategy, has evolved but retained its core principles across different historical periods. The research adopts a qualitative analytical approach, drawing upon classical texts, modern theoretical frameworks, and contemporary digital practices. It argues that the Trojan Horse is not merely a mythological construct but a continuing reality in modern society, particularly in the digital age where cyber threats exploit human psychology

and trust. The study further highlights how political and economic systems often employ Trojan-like strategies to achieve influence and control. The findings suggest that the persistence of this metaphor is deeply rooted in human behavior, especially the tendency to trust external appearances. The article concludes that awareness, critical thinking, and ethical responsibility are essential tools to counter modern forms of deception. The Trojan Horse, therefore, remains a timeless symbol that bridges the past, present and future, offering valuable insights into both human nature and contemporary global challenges.

KEYWORDS: Odyssey, Myths, Deception, Cyber Security, Strategy, Mythology, Digital Threats, Trust

تعارف:

انسانی تاریخ میں فریب، تدبیر، اور حکمتِ عملی ہمیشہ سے مرکزی حیثیت رکھتے ہیں۔ قدیم جنگوں سے لے کر جدید ڈیجیٹل دنیا تک، انسان نے اپنی بقا اور کامیابی کے لیے اکثر ایسی چالیں اختیار کی ہیں جن میں ظاہری دوستی یا اعتماد کے پیچھے کوئی پوشیدہ مقصد کارفرما ہوتا ہے۔ انہی چالوں میں سب سے مشہور ٹروجن ہارس (Trojan Horse) ہے، جو نہ صرف یونانی اساطیر کا ایک لازوال واقعہ ہے بلکہ آج کی سائبر سیکیورٹی (Cybersecurity) کی دنیا میں بھی بطورِ استعارہ زندہ ہے۔

''ٹروجن ہارس'' کی اصطلاح اس وقت استعمال ہوتی ہے جب کوئی چیز بظاہر مفید یا بے ضرر دکھائی دے، مگر دراصل اس کے اندر کوئی خطرناک یا نقصان دہ عنصر چھپا ہو۔ یہ تصور اس حد تک مضبوط ہے کہ اس نے ادب، سیاست، عسکری حکمتِ عملی، اور ٹیکنالوجی کے مختلف شعبوں کو متاثر کیا ہے۔ قدیم یونان کے زمانے میں یہ محض ایک جنگی چال تھی، لیکن جدید دور میں یہ ڈیجیٹل فریب (Digital Deception) کی علامت بن چکی ہے۔ آج کے دور میں، کمپیوٹر نیٹ ورکس اور انفارمیشن سسٹمز میں ہونے والے سائبر حملے، خاص طور پر ٹروجن ضرر رساں سافٹ ویئر یا مالویئر (Trojan

(Malware)، اسی تاریخی کہانی کے جدید ورژن ہیں۔ اس لیے ٹروجن ہارس نہ صرف ماضی کی ایک داستان ہے بلکہ موجودہ دور کے خطرات کی تعبیر بھی ہے۔

اس تحقیق کا مقصد اس اس زرمیہ کہانی کے ارتقائی سفر کو واضح کرنا ہے کہ کس طرح ایک 800 ق م قدیم حکمتِ عملی جدید دنیا کے لیے استعارہ بن گئی۔ اس تحقیق کے سلسلے میں پہلے اساطیری پس منظر بیان کیا جائے گا، پھر یہ دیکھا جائے گا کہ یہ تصور کیسے ادب، سیاست، معیشت، اور سائبر سیکیورٹی میں منتقل ہوا، اور آخر میں اس کے اخلاقی و سماجی مضمرات پر غور کیا جائے گا۔ اس سلسلے میں تفصیل سے ہر چیز بیان کی گئی ہے۔

ٹرائے کی جنگ کی بنیاد:

یونانی اساطیر کے مطابق ٹرائے کی جنگ کی بنیاد ایک نہایت علامتی اور اخلاقی سبق رکھنے والے واقعے سے پڑی، جس کا آغاز دیوتاؤں کی ایک شادی سے ہوا۔ کہا جاتا ہے کہ سمندری دیوی تھیٹس (Thetis) اور فانی انسان پیلیوس (Peleus) کی شادی میں تمام دیوتاؤں اور دیویوں کو مدعو کیا گیا، سوائے ایرس (Eris) دیوی کے جو جھگڑے، حسد اور انتشار کی دیوی سمجھی جاتی تھی۔ چونکہ دیگر دیوتا اس کے فساد انگیز رویّے سے نالاں تھے، اس لیے اسے جان بوجھ کر شادی کی تقریب میں نہیں بلایا گیا تھا۔ ایرس نے اس توہین کو قبول نہ کیا اور بدلہ لینے کا فیصلہ کیا۔ وہ خاموشی سے شادی کی محفل میں داخل ہوئی اور ایک سنہری سیب (Golden Apple) پھینک گئی، جس پر یونانی زبان میں لکھا تھا ''سب سے خوبصورت کے لیے''۔ یہ سیب دیکھتے ہی تین عظیم دیویاں ہیرا (Hera)، ایتھینا (Athena) اور ایفروڈائٹی (Aphrodite) اس بات پر جھگڑنے لگیں کہ سیب کی حقدار کون ہے، کیونکہ ہر ایک خود کو سب سے زیادہ خوبصورت سمجھتی تھی۔ اس جھگڑے کا فیصلہ کرنے کے لیے دیوتاؤں کے بادشاہ زیوس (Zeus) نے فیصلہ کرنے سے انکار کر دیا اور یہ ذمہ داری پیرس (Paris) کے سپرد کر دی، جو ٹرائے کا شہزادہ تھا۔ تینوں دیویوں نے پیرس کو رشوت دینے کی کوشش کی

- ہیرا نے اقتدار اور بادشاہت کا وعدہ کیا،
- ایتھینا نے عقل اور جنگی فتح کی پیشکش کی،
- جبکہ ایفروڈائٹی نے دنیا کی سب سے خوبصورت عورت کا وعدہ کیا۔

پیرس نے ایفروڈائٹی کا انتخاب کیا، جس کے نتیجے میں اسے دنیا کی سب سے خوبصورت عورت ہیلن (Helen) ملی، جو اسپارٹا کے بادشاہ مینیلاؤس (Menelaus) کی بیوی تھی۔ پیرس ہیلن کو اپنے ساتھ ٹرائے لے آیا، اور یہی واقعہ بعد میں ٹرائے کی جنگ کا سبب بنا۔ یوں ایک دیوی کو نظر انداز کرنا، ایک سنہری سیب، اور حسد و فریب نے مل کر ایسی جنگ کو

جنم دیا جو یونانی تاریخ اور اساطیر میں ہمیشہ کے لیے امر ہو گئی۔ یہ کہانی اس بات کی علامت ہے کہ معمولی سمجھا جانے والا فریب بھی تاریخ کا رخ بدل سکتا ہے۔

اس کے بعد یونانیوں کے بادشاہ اور ٹرائجن (Trojans) کے درمیان ایک طویل جنگ جاری تھی، جسے ٹرائے کی جنگ (Trojan War) کہا جاتا ہے۔ دس سال کی لڑائی کے باوجود، یونانی فوج ٹرائے شہر کو فتح کرنے میں ناکام رہی کیوں کہ اس شہر کی دیواریں مضبوط اور ناقابلِ تسخیر تھیں۔ ٹروجن ہارس کی کہانی یونانی اساطیر (Greek Mythology) کا ایک مشہور واقعہ ہے جو ایلیڈ (Iliad) اور اوڈیسی (Odyssey) جیسی ادبی تخلیقات میں بھی بیان ہوا ہے۔ اس بارے سے Murphy Lauren اپنے آرٹیکل میں ہومر کا حوالہ دے کر لکھتے ہیں :

> The horse of myth is used to penetrate the walls of Troy and seize the city by trickery as described by the epic poet, [Homer Od. 4.271–4.289, 8.492–520] (1)

اساطیر میں بیان کیا گیا گھوڑا ٹرائے کی فصیلوں کو چیر کر اندر داخل ہونے اور فریب کے ذریعے شہر پر قبضہ کرنے کے لیے استعمال ہوا، جیسا کہ ہومر نے بیان کیا ہے(1) [Od. 4.271–4.289, 8.492–520]

بالآخر، یونانی کمانڈر ''اوڈیسیس (Odysseus)'' نے ایک غیر روایتی منصوبہ تیار کیا۔ اوڈیسیس کے منصوبے کے مطابق ایک دیو ہیکل لکڑی کا گھوڑا تیار کیا گیا، جو بظاہر یونانیوں کی شکست کی علامت تھا اور ٹرائجن کو بطور تحفہ پیش کیا گیا تھا۔ یونانی فوج نے ظاہراً پسپائی اختیار کی، اور گھوڑا میدانِ جنگ میں چھوڑ دیا۔ ٹرائجن شہری اسے دشمن کی شکست کی علامت سمجھ کر شہر کے اندر لے آئے۔ مگر رات کے وقت، اس گھوڑے کے اندر چھپے ہوئے یونانی سپاہی باہر نکلے، شہر کے دروازے کھولے، باہر چھپی فوج کو اندر بلایا اور شہر پر حملہ کر کے ٹرائے کو مکمل طور پر تباہ کر دیا۔

یہ واقعہ بظاہر ایک جنگی فریب تھا، مگر اس کے اثرات علامتی سطح پر بہت گہرے ہیں۔ ''ٹروجن ہارس'' انسانی تاریخ میں دھوکے اور اعتماد کے غلط استعمال کی سب سے قدیم مثال بن گیا۔ اس کہانی میں ''اعتماد'' اور ''تدبیر'' کے درمیان وہ باریک لکیر نمایاں ہوتی ہے جو دشمن کو دوست کے بھیس میں پیش کرتی ہے۔

علامتی طور پر، ٹروجن ہارس اس بات کی نمائندگی کرتا ہے کہ خطرہ ہمیشہ کھلے عام ظاہر نہیں ہوتا بلکہ اکثر دوست یا مددگار کے روپ میں سامنے آتا ہے۔ یہ واقعہ انسان کو یہ سکھاتا ہے کہ ظاہری خیر خواہی ہمیشہ حقیقت نہیں ہوتی۔ اسی علامت نے وقت گزرنے کے ساتھ ساتھ مختلف میدانوں میں نئی شکلیں اختیار کیں۔ ادب میں اسے ''دھوکہ دہی کے فن'' کے

طور پر بیان کیا گیا، سیاست میں اسے ''پوشیدہ ایجنڈوں'' کی علامت کے طور پر اپنایا گیا، اور ٹیکنالوجی میں یہ مالویئر (Malware) کے بنیادی تصور کی بنیاد بنا۔

جدید دنیا میں، جب کمپیوٹر نیٹ ورکس میں ٹروجن ضرر رساں سافٹ ویئر داخل ہوتا ہے تو وہ بالکل اسی اصول پر کام کرتا ہے- بظاہر ایک مفید یا غیر نقصان دہ فائل کی صورت میں، مگر دراصل اندر سے نقصان دہ کوڈ چھپا ہوتا ہے جو سسٹم کی سکیورٹی کو کمزور کر دیتا ہے۔ یوں کہا جا سکتا ہے کہ قدیم ٹرائے کی جنگ کا وہ لکڑی کا گھوڑا آج "ڈیجیٹل دنیا" میں دوبارہ جنم لے چکا ہے، جہاں وہ کوڈ اور ڈیٹا کے ذریعے حملہ کرتا ہے نہ کہ تلوار اور نیزے کے ذریعے۔

آج کی دنیا میں اگر ہم ٹروجن ہارس کے تصور کو دیکھیں تو اس کا واضح مظہر Email Attachments یا Fake Software Updates کی صورت میں نظر آتا ہے۔ مثال کے طور پر 2017 میں سامنے آنے والا Emotet Trojan ایک ایسا مالیشئس پروگرام (malicious program) تھا جو invoice یا payment document کے بھیس میں بھیجا جاتا تھا۔ جیسے ہی صارف اسے کھولتا تو وہ خود بخود سسٹم میں انسٹال ہو کر بینکنگ معلومات چرانے لگتا۔ یہ عمل بالکل اسی طرح تھا جیسے ٹرائجن نے یونانیوں کے لکڑی کے گھوڑے کو شہر میں داخل ہونے دیا تھا۔ اور داخل ہونے کے بعد قبضہ کر کے ٹارجن کو یونانیوں نے تباہ کر دیا تھا اور فتح حاصل کی گئی تھی اس حکمت عملی کے تحت آج بھی یہ تدبیر اختیار کی جاتی ہے مختلف طریقوں سے اسے استعمال کر کے فائدے حاصل کیے جاتے ہیں جس سے یہ بات ظاہر ہوتی ہے کہ دشمن ہمیشہ ظاہری حملہ نہیں کرتا بلکہ دوستی یا تحفے کی صورت میں اندر داخل ہو کر نقصان پہنچاتا ہے-

ٹروجن ہارس کا اساطیری پس منظر:

یونانی اساطیر میں ٹروجن ہارس کی کہانی دنیا کی سب سے مشہور حکایات میں شمار ہوتی ہے- یہ انسانی تاریخ کی قدیم ترین فکری میراث ہے، جو نہ صرف قدیم جنگی حکمتِ عملیوں کی علامت ہے بلکہ انسانی ذہانت، فریب، اعتماد اور طاقت کی لازوال علامت بھی ہے۔ یہ واقعہ ''ایلیڈ'' اور ''اوڈیسی'' جیسے قدیم یونانی ادب کے شاہکاروں میں بیان ہوا ہے، جنہیں شاعر ہومر (Homer) سے منسوب کیا جاتا ہے۔ یونانی ادب میں ٹروجن ہارس کو عقل و فریب کے امتزاج کی علامت سمجھا جاتا ہے جہاں ایک طرف یہ انسانی ذہانت کی فتح ہے وہاں یہ اعتماد کے غلط استعمال اور اندرونی کمزوری کی بھی نشاندہی کرتا ہے- ہومر نے ایلیڈ میں براہ راست اس کا ذکر نہیں کیا، اوڈیسی میں بھی محدود ذکر ملتا ہے اور وہاں بھی یہی بات ظاہر ہوتی ہے کہ طاقتور بھی اپنی عقل کے فریب میں آکر برباد ہو سکتا ہے-

علامتی معنی: اعتماد، دھوکہ اور ٹرائے کا زوال:

ٹروجن ہارس کی کہانی بظاہر ایک جنگی چال ہے، مگر دراصل یہ انسانی نفسیات اور سماجی اعتماد کے ٹوٹنے کی ایک استعاراتی کہانی (metaphorical narrative) ہے۔

• اعتماد: ٹرائجن باشندوں نے دشمن کے تحفے پر یقین کیا اور اس اعتماد نے اُن کی تباہی کا راستہ ہموار کیا۔

• دھوکہ: دشمن نے طاقت کے بجائے فریب کو ہتھیار بنایا، یعنی ذہانت نے قوت پر غلبہ پایا۔

• زوال: ٹرائے کی تباہی دراصل اُس لمحے شروع ہوئی جب اعتماد نے احتیاط کی جگہ لے لی۔

یہی وہ نکتہ ہے جو اس کہانی کو ابدی بناتا ہے، ایک ایسا سبق جو صدیوں بعد بھی سیاست، کاروبار، تعلقات، اور سائبر سیکیورٹی جیسے جدید میدانوں میں لاگو ہوتا ہے۔

ٹروجن ہارس کو تاریخ میں محض ایک جنگی چال نہیں بلکہ ایک عالمی استعارہ (universal metaphor) سمجھا جاتا ہے۔ اس کا مفہوم یہ ہے کہ خطرہ ہمیشہ ظاہر نہیں ہوتا، بعض اوقات وہ ایک دلکش صورت میں چھپا ہوتا ہے۔ یہ استعارہ اس بات کی یاد دہانی ہے کہ انسانی معاشرہ ہمیشہ کسی نہ کسی شکل میں اعتماد کے غلط استعمال کا شکار رہا ہے۔ یعنی یہ کہانی تاریخی واقعہ نہیں بلکہ انسانی تجربے، نفسیات اور تہذیبی رویوں کی آفاقی علامت بن گئی ہے۔ یہ ہمیں بتاتا ہے کہ انسان خود اپنی عقل اور اعتماد کی غلط استعمال سے تباہ ہو سکتا ہے۔

تاریخی اور ادبی اثرات:

اس کہانی نے بعد کے ادوار میں مختلف تہذیبوں، ادبی تخلیقات، اور فلسفیانہ مباحث کو متاثر کیا۔

• رومی شاعر ورجل (Virgil) نے اپنی شہرہ آفاق نظم "Aeneid" میں اس واقعے کو امر کر دیا۔

• رینیسنس (Renaissance) کے بعد کے مصوروں اور ڈرامہ نگاروں نے اسے انسانی فریب اور قسمت کے تعلق کے طور پر پیش کیا۔

• شیکسپیئر کے ڈراموں سے لے کر جدید ناولوں تک، ٹروجن ہارس کی علامت انسانی فریب، دوغلے پن، اور طاقت کے کھیلوں کی نمائندگی کرتی ہے۔ مثال کے طور پر، جارج آرویل کے ناول اینمل فارم میں طاقت کے نام پر عوام کو گمراہ کرنے کا تصور ایک ٹروجن کے منصوبے (Trojan Strategy) کی صورت میں ظاہر ہوتا ہے۔

ٹروجن ہارس کا اساطیری پس منظر صرف ایک قدیم واقعہ نہیں بلکہ انسانی رویوں، سیاسی چالوں، اور نفسیاتی فریب کی ایک آفاقی تمثیل ہے۔ اس نے دنیا کو یہ سکھایا کہ ہر خطرہ واضح نہیں ہوتا، اکثر دشمن ایک ''تحفہ'' بن کر آتا ہے۔ یہی فلسفہ آج کے ڈیجیٹل عہد (digital age) میں بھی اتنا ہی متعلق ہے جتنا کہ قدیم ٹرائے کے میدان میں تھا۔ اردو ادب میں باقاعدہ اس نام سے کہانیاں یا شاعری نہیں ملتی مگر کچھ افسانے اور کہانیوں میں فریب اور دھوکہ دہی کے مختلف حربے دکھائے گئے ہیں جو علامتی طور پر ٹروجن ہارس کے اثرات کو ظاہر کرتے ہیں اس میں منٹو، قراۃ العین، حیدر وغیرہ کے ناول اور افسانے خوبصورتی کے پیچھے چھپے دھوکے کے بارے میں بتاتے ہوئے نظر آتے ہیں۔

قدیم ٹرائے سے جدید دنیا تک:

وقت گزرنے کے ساتھ ٹروجن ہارس نے اپنی شکل بدل لی، لیکن اس کا جوہر، اعتماد کے اندر چھپا خطرہ، آج بھی اتنا ہی متعلقہ ہے۔ جدید دنیا میں یہ تصور مختلف شعبوں جیسے کہ سیاسیات، اقتصادیات، ٹیکنالوجی، میڈیا، صحافت اور فوجی حکمت عملی میں نئے معانی کے ساتھ ظاہر ہوتا ہے۔

جدید دور میں ٹروجن ہارس جیسی حکمتِ عملیوں کا استعمال:

قدیم یونان کی عسکری حکمتِ عملی آج کے زمانے میں Psychological ، Strategic Manipulation Operations (PsyOps)، اور Hybrid Warfare کے صورات میں زندہ ہے۔ جدید ریاستیں اور ادارے اکثر کسی ملک، کمپنی یا فرد کے اعتماد کو استعمال کر کے اندر سے اثر انداز ہونے کی کوشش کرتے ہیں۔ مثال کے طور پر سرد جنگ کے دوران سوویت یونین اور امریکہ نے ایک دوسرے کے اندر ثقافتی ٹروجن ہارس (Cultural Trojan Horses) پیدا کیے جیسے فلم، ادب، اور میڈیا کے ذریعے نظریاتی اثر قائم کرنا۔

سیاست میں استعمال:

بین الاقوامی تعلقات میں، ایک ملک دوسرے ملک میں امداد یا دوستی کے بہانے اپنے اثرات قائم کرنے کی کوشش کرتا ہے۔ مثال کے طور پر، بعض ترقی پذیر ممالک میں بڑی طاقتیں انفراسٹرکچر پروجیکٹس کے ذریعے Strategic Access حاصل کرتی ہیں۔ ریاستیں یا جماعتیں اکثر اپنے مخالفین کے اندر Soft Influence Tools کے ذریعے اثر انداز ہونے کی کوشش کرتی ہیں۔ پروپیگنڈا، Fake Narratives، یا انسانی امداد (Humanitarian Aid) کے پردے میں سیاسی مفادات حاصل کرنا ایک جدید ٹروجن حکمتِ عمل (Trojan Tactic) بن چکا ہے۔

سفارت کاری میں استعمال:

جدید سیاست میں دھوکہ دہی پر مبنی سفارتکاری (Trojan Diplomacy) ایک اصطلاح کے طور پر استعمال ہوتی ہے، جس سے مراد وہ پالیسی ہے جس کے ذریعے کوئی ملک بظاہر تعاون کی پیشکش کرتا ہے لیکن دراصل معلومات جمع کرنا (Intelligence Gathering) یا اثر و رسوخ قائم کرنا (Influence Building) کر رہا ہوتا ہے۔ یہی اصول مختلف بین الاقوامی NGOs یا میڈیا نیٹ ورکس پر بھی لاگو ہوتا ہے جو بظاہر فلاحی مقاصد رکھتے ہیں مگر اصل میں مخصوص جیوپولیٹیکل مقاصد (Geopolitical Objectives) کے لیے کام کر رہے ہوتے ہیں۔

کاروبار میں استعمال:

عالمی کاروبار میں کارپوریٹ گھس بیٹھ کی حکمت عملی (Corporate Trojan Strategies) عام ہو چکی ہیں۔ بڑی کمپنیاں مارکیٹ میں کم قیمت پر داخل ہو کر بعد میں مقامی صنعتوں کو ختم کر دیتی ہیں۔ کاروباری دنیا میں برانڈ ٹروجن کی حکمت عملی (Brand Trojan Strategies) کا رجحان بڑھ رہا ہے یعنی کمپنی بظاہر صارف کے فائدے کے لیے کام کرتی ہے مگر اندرونی طور پر ڈیٹا مائننگ (Data Mining)، نفسیاتی پروفائلنگ (Psychological Profiling)، یا عملیاتی طرز عمل کی پیش گوئی (Behavioral Prediction) کے مقاصد رکھتی ہے۔

میڈیا میں استعمال:

سوشل میڈیا کے دور میں Fake Accounts یا Bot Networks کو عوامی رائے پر اثر ڈالنے کے لیے استعمال کیا جاتا ہے۔ یہ ایک جدید ٹروجن ہارس ہے جو ذہنوں کو متاثر کرتا ہے۔ اسی طرح میڈیا میں گمراہ کن خبریں کی مہم (Disinformation Campaigns)، اور بااثر بیانیے (Influencer Narratives) کے ذریعے عوامی رائے کو تبدیل کرنا ایک ٹرائجن طرزِ حکمتِ عملی ہے۔ میڈیا میں اس کا مطلب کسی چیز کو خوبصورت کر کے دکھانا مگر اس کے اندر پوشیدہ خاص مقاصد چھپے ہوتے ہیں، بظاہر فن یا خوشی دکھانا مگر اس کے پیچھے مقصد چھپا ہوتا ہے، کسی خاص پروڈکٹ کو بار بار دکھانا یعنی باہر کے پروڈکٹس کو زیادہ فروغ دینا، خبروں اور ٹاک شو وغیرہ میں کوئی ایسی خبر دکھانا یا کسی ایسی خبر کے بارے میں بات کرنا، جس سے کسی ملک کے حوالے سے منفی رجحان پیدا ہو پولیٹیکل میمز بنا کر لوگوں کا رجحان دوسری طرف کرنا، یعنی ہنسی مذاق کے پیچھے لوگوں کی توجہ دوسری طرف مبذول کروانا۔

ٹیکنالوجی اور مصنوعی ذہانت میں ٹروجن اصول:

ٹیکنالوجی کے میدان میں ٹروجن ہارس کی اصطلاح سب سے زیادہ سائبر سیکیورٹی اور مصنوعی ذہانت (Artificial Intelligence) کے تناظر میں استعمال ہوتی ہے۔ جدید مالویئر اکثر Trojan Mechanism پر مبنی ہوتا ہے یعنی ایک ایسا پروگرام جو بظاہر بے ضرر لگے مگر اندر خفیہ مضر کوڈ (Malicious Code) رکھتا ہو۔ مصنوعی ذہانت کے

اس دور میں Algorithmic Manipulation ایک نیا ٹروجن ہارس ہے۔ صارفین کو یہ یقین دلایا جاتا ہے کہ وہ آزادانہ طور پر فیصلہ کر رہے ہیں، جبکہ درحقیقت ان کے انتخاب پہلے سے ہی Data-driven Biases کے ذریعے متعین کیے جا چکے ہوتے ہیں۔

سائبر سیکیورٹی میں ٹروجن ہارس:

جدید دنیا میں ٹروجن ہارس کا سب سے واضح اور عملی اطلاق سائبر سیکیورٹی کے میدان میں نظر آتا ہے۔ جس طرح قدیم ٹرائے کے شہریوں نے ایک خوبصورت گھوڑے کو فتح کی علامت سمجھ کر شہر کے اندر داخل کر لیا تھا، اسی طرح آج کے ڈیجیٹل صارفین اکثر ایک بظاہر محفوظ فائل، سافٹ ویئر، یا لنک کو کھول کر اپنے سسٹم میں مالویئر داخل کر دیتے ہیں۔ یہی جدید سائبر ٹروجن ہے، ایک پرانا فریب، لیکن نئے ڈیجیٹل لباس میں۔

سائبر ٹروجن کی تعریف اور طریقۂ کار:

ایک سائبر ٹروجن دراصل ایسا مالیشئس پروگرام ہوتا ہے جو مستند سافٹ ویئر (Legitimate Software) کا روپ دھار لیتا ہے تاکہ صارف کو دھوکے میں ڈال سکے۔ یہ بظاہر فائدہ مند لگتا ہے مگر اندرونی طور پر یہ سسٹم کی سکیورٹی کی پرتھ (Security Layer) کو نظر انداز کر کے غیر مستند طریقے سے رسائی حاصل کر لیتا ہے مثلاً کوئی سافٹ ویئر اپ ڈیٹ، یا ای میل Email Attachment ۔ یہ ٹرائجن ایک بار سسٹم میں داخل ہو جائے تو یا تو حساس معلومات چُرا لیتا ہے، یا خفیہ راستہ (Backdoor Entry) بنا کر ہیکر کو سسٹم کی مکمل کنٹرول دے دیتا ہے۔ اس کے بعد وہ ہیکر سسٹم کی نگرانی، غلط استعمال یا چھیڑ چھاڑ کر سکتا ہے، بالکل اسی طرح جیسے یونانی سپاہیوں نے ٹرائے کے گھوڑے کے اندر سے نکل کر شہر پر قبضہ کر لیا تھا۔

ٹروجن سسٹمز میں داخل کیسے ہوتے ہیں؟:

ٹروجن ہارس عام طور پر درج ذیل طریقوں سے کمپیوٹر یا نیٹ ورک میں داخل ہوتے ہیں:

• جھوٹی یا دھوکہ دہی والے ای میلز (Phishing Emails) جو کسی معتبر ادارے کی معلوم ہوتی ہیں مگر دراصل مالیشئس لنک رکھتی ہیں۔

• جعلی سافٹ ویئر ڈاؤن لوڈ: (Fake Software Downloads) یہ ایسے ایپس یا اپڈیٹس ہوتے ہیں جو بظاہر یوٹیلیٹی سافٹ ویئر لگتے ہیں لیکن اصل میں مالویئر ہوتے ہیں۔

•سوشل انجینئرنگ: انسانی نفسیات کو استعمال کرتے ہوئے صارف کو تجسس یا فوری ضرورت کا احساس دلا کر کسی لنک یا بٹن پر کلک کروانا۔

•متاثرہ (compromised) ویب سائٹس: ایسی مالیشس ویب سائٹس جو صارف کے کھولتے ہی خودکار طریقے سے ٹروجن کو سسٹم میں داخل کر دیتی ہیں۔

ٹروجن کی اقسام:

•بیک ڈور ٹروجنز :(Backdoor Trojans) یہ سسٹم میں ایک خفیہ راستہ (Backdoor) بنا دیتے ہیں جس کے ذریعے ہیکر بار بار اور بغیر اجازت سسٹم تک رسائی حاصل کر سکتا ہے۔ کسی سافٹ ویئر فائل گیم یا ای میل وغیرہ کے ذریعے آتا ہے صارف کوئی عام سی چیز سمجھ کر انسٹال کر لیتا ہے اور یہ خاموشی سے اپنا خفیہ راستہ بنا لیتا ہے اور کبھی بھی کمپیوٹر میں داخل ہو سکتا ہے فائلیں چوری، کاپی، یا ڈیلیٹ کر سکتا ہے، پاسورڈ چوری کر سکتا ہے اور اس کے ذریعے نقصان پہنچا سکتا ہے۔

•بینکنگ ٹروجنز :(Banking Trojans) یہ صارف کی مالی معلومات مثلاً اے ٹی ایم پن، کریڈٹ کارڈ تفصیلات، او ٹی پی اور آن لائن بینکنگ اسناد کو چوری کر کے مجرمانہ مقاصد کے لیے استعمال کرتے ہیں۔

•اسپائی ویئر ٹروجنز :(Spyware Trojans) یہ خفیہ طور پر صارف کی سرگرمیوں اور دیگر معلومات کی نگرانی کر کے انہیں ہیکر تک منتقل کرتے ہیں۔

•رینسم ویئر ٹروجنز :(Ransomware Trojans) یہ متاثرہ نظام یا ڈیٹا کو لاک یا انکرپٹ کر دیتے ہیں اور بحالی کے بدلے تاوان (Ransom) کا مطالبہ کرتے ہیں، بصورتِ دیگر ڈیٹا مستقل طور پر ضائع ہونے کا خطرہ ہوتا ہے۔

•چارجر ٹروجن:(Charger Trojan) یہ ٹروجن ایسے عام موبائل چارجرز میں شامل کیا جاتا ہے جو بظاہر عام نظر آتے ہیں، لیکن اندر موجود malicious micro-chip موبائل ڈیوائس کو چارج ہونے کے دوران متاثر کر دیتی ہے اور خفیہ طور پر ڈیٹا چوری یا سسٹم کی نگرانی کا عمل انجام دیتی ہے.

•چپ ٹروجن :(Chip Trojan) مادر بورڈ یا پروسیسر کی چپ میں خفیہ کوڈ شامل کر کے سسٹم پر مستقل کنٹرول حاصل کیا جاتا ہے۔

•اسمارٹ اسپیکر ٹروجن :(Smart Speaker Trojan) اسپیکر یا وائس اسسٹنٹ میں ایسا کوڈ شامل کیا جاتا ہے جو گفتگو یا آواز ریکارڈ کر کے ہیکر تک پہنچاتا ہے۔

•کیمرہ ٹروجن :(Camera Trojan) ویڈیو یا سی سی ٹی وی کیمروں میں موجود سافٹ ویئر کو متاثر کر کے لائیو ویڈیو چوری کی جاتی ہے۔

•اسمارٹ واچ ٹروجن :(Smartwatch Trojan) گھڑی کے اندر موجود سافٹ ویئر میں داخل ہو کر صارف کی صحت، مقام اور میسجز چوری کرتا ہے۔

•یو ایس بی ٹروجن :(USB Trojan) متاثرہ یو ایس بی ڈرائیو سسٹم میں لگتے ہی خودکار طور پر مالیشئس پروگرام انسٹال کرتی ہے۔ یو ایس بی ٹارجن سے مراد یو ایس بی میں چھپا ایسا وائرس جو کمپیوٹر میں لگاتے ہی کمپیوٹر خراب کر دیتا ہے اور اس کا سارا ڈیٹا چرا لیتا ہے۔

•کیو آر کوڈ ٹروجن :(QR Code Trojan) جعلی کیو آر کوڈ اسکین کرنے پر صارف کو مالیشئس ویب سائٹ پر لے جاتا ہے یا فون میں مالویئر انسٹال کرتا ہے۔

•مشینری پارٹس ٹروجن :(Machine Hardware Trojan) صنعتی مشینوں یا فیکٹری سسٹمز کے پرزوں میں خفیہ نقصان دہ سرکٹس شامل کیے جاتے ہیں۔

•سگریٹ باکس ٹروجن :(Cigarette Pack Trojan) کسٹمز اور سیکیورٹی کو دھوکہ دینے کے لیے سگریٹ ڈبوں میں چھپے ہوئے اسپائینگ آلات استعمال کیے جاتے ہیں۔

•کھلونوں میں ٹروجن :(Toy Trojan) بچوں کے اسمارٹ کھلونوں میں مائیکروفون یا سینسر کے ذریعے خفیہ نگرانی اور معلومات جمع کی جاتی ہے۔

•پاور بینک ٹروجن :(Power Bank Trojan) متاثرہ پاور بینک موبائل چارج ہوتے وقت ڈیٹا چوری یا مالویئر انسٹال کر دیتا ہے۔

•جعلی کوریئر ایس ایم ایس ٹروجن :(Fake Courier SMS Trojan) یہ ٹروجن عام طور پر کوریئر یا پارسل ڈلیوری کے نام سے موصول ہونے والے جعلی پیغامات کے ذریعے پھیلایا جاتا ہے۔ ان ایس ایم ایس میں موجود مالیشئس لنک پر کلک کرنے سے موبائل فون یا کمپیوٹر متاثر ہو جاتا ہے اور نظام میں مالویئر داخل ہو کر حساس معلومات کی چوری یا دیگر نقصان دہ سرگرمیوں کا آغاز کر دیتا ہے۔

• گفٹ باکس ٹروجن: تحفے کے طور پر دیا جانے والے اشیاء بظاہر نارمل ہوتا ہے لیکن اندر خفیہ نگرانی کے آلات لگی ہوتی ہے۔ بعض اوقات گفٹ باک کسی دشمن کو دیا جاتا ہے جسے کھولتے ہی دھماکہ ہوتا ہے اور موقع پر موت بھی واقع ہو جاتی ہے یا کوئی بڑا نقصان ہو جاتا ہے۔

• ڈرون کیمرہ ٹارجن: جسے توڑنے کی صورت میں اس کے اندر موجود مزید ڈرون کیمرے نکل کر ہر طرف پھیل جاتے ہیں

ہیکرز کے ذریعہ فریب دے کر سسٹمز میں داخل ہونے کے طریقے

یہ ٹرائجن انسانی کمزوریوں کو ہدف بناتے ہیں، تکنیکی کمزوریوں کو نہیں۔ ہیکرز عموماً خوف، تجسس، اور اعتماد کا استحصال کرتے ہیں-مثلاً "Click here to win a prize" یا "Update your security settings" جیسے جملے وہ ٹرائجن کو داخل کرنے کے لیے استعمال کرتے ہیں۔ اس طرح ٹرائجن ایک نفسیاتی فریب بھی ہے، صرف تکنیکی خطرہ نہیں۔ اس حوالے سے Raymond Gozzi اور Bruce Meyerson لکھتے ہیں:

> A Trojan Horse named "Explore. Zip" made headlines in June, 1999. It was first detected in Israel, but in less than a week had spread around the world. It erased files on tens of thousands of corporate computers at AT&T, Boeing, General Electric, Micro soft, and perhaps others (2,3).
>
> This Trojan Horse arrived as an attachment to an e-mail message. The e-mail message came from the computer of someone you knew, and stated "I received your e-mail and I shall send you a reply ASAP. Til then, take a look at the attached zipped docs." The attached file, named "zipped-files.exe" contained the Trojan Horse. (An "exe" suffix means the file is executable, in other words, a program which will run on your machine (2).

جدید دفاعی اقدامات اور صارفین کی آگاہی کی حکمتِ عملی:

سائبر ٹروجن سے بچاؤ کے لیے کثیر سطحی حفاظتی حکمت عملی (Multi-layered Security Approach) ضروری ہے:

•اینٹی وائرس اور فائروال سسٹمز :(Antivirus & Firewall Systems) یہ نظام مستقل طور پر سسٹم کی اسکیننگ کرتا ہے اور مشکوک فائلز کو قرنطینہ (Quarantine) میں ڈال دیتا ہے تاکہ کسی بھی مالویئر کے پھیلاؤ کو روکا جا سکے۔

•صارف کی تعلیم :(User Education) عوام میں آگاہی پیدا کرنا ضروری ہے کہ ہر ای میل یا ڈاؤن لوڈ محفوظ نہیں ہوتا اور ہر لنک پر بلا سوچے کلک کرنا خطرناک ہو سکتا ہے۔

Behavioral Analysis Toolsایسے سافٹ ویئر استعمال کیے جائیں جو ٹروجن کی غیر معمولی سرگرمیوں کی کھوج کر سکیں اور فوری طور پر الرٹ جاری کریں۔

•باقاعدہ اپڈیٹس :(Regular Updates) پرانا سافٹ ویئر ٹروجن کے لیے آسان ہدف بن جاتا ہے، اس لیے سسٹمز اور ایپلیکیشنز (Applications) کو ہمیشہ اپڈیٹ رکھنا لازمی ہے۔

•زیرو ٹرسٹ آرکیٹیکچر :(Zero-Trust Architecture) کسی بھی سسٹم کے جزو (System Component) پر اندھا اعتماد نہ کیا جائے، بلکہ ہر عنصر کی آزادانہ اور مستقل تصدیق (Independent Verification) ضروری ہے۔

جدید دور میں ٹروجن ہارس صرف ایک تکنیکی اصطلاح نہیں بلکہ ایک سائبر فلسفہ(Cyber Philosophy) ہے جو ہمیں یہ سکھاتی ہے کہ خاص طور پر ڈیجیٹل دنیا میں اندھا اعتماد نہیں ہونا چاہیے۔

فوجی واسٹریٹجک استعمال:

ٹروجن ہارس کا تصور صرف اساطیر (Mythology) یا سائبر اسپیس (Cyberspace) تک محدود نہیں، بلکہ عالمی سطح پر عسکری حکمتِ عملی (Military Strategy) اور خفیہ کارروائیوں (Intelligence Operations) کے بنیادی اصولوں میں شامل ہے۔ قدیم یونانیوں کے اس جنگی فریب نے عسکری تاریخ میں فریب پر مبنی جنگی طرزِ عمل (Deception-based Warfare)کا مستقل تصور پیدا کیا، جس کا مقصد دشمن کو براہِ راست طاقت سے نہیں بلکہ اس کے اعتماد کو ہتھیار بنا کر شکست دینا تھا۔

فریب اور دھوکے پر مبنی تاریخی جنگی حربے

تاریخ میں کئی مشہور جنگیں ٹرائجن طرز کے فریب پر مبنی رہیں:

• دوسری عالمی جنگ میں برطانوی فوج نے Operation Fortitude کے نام سے ایک مکمل جعلی فوجی دستہ تیار کیا، تاکہ جرمن فوج کو ڈی ڈے (D-Day) کے اصل مقام سے گمراہ کیا جاسکے۔ یہ ایک جدید ٹروجن حکمتِ عملی تھی۔

• سرد جنگ کے دوران، دونوں سپر پاورز نے ایک دوسرے کے اندر ثقافتی، تعلیمی اور ذرائع ابلاغ میں رسوخ کے ذریعے نظریاتی اثر و رسوخ بڑھایا۔ یہ ٹروجن اثر و نفوذ جدید دور کی نفسیاتی جنگ تھی۔

• آپریشن منس میٹ (Operation Mincemeat) میں برطانوی خفیہ ادارے نے ایک لاش کے ذریعے جعلی دستاویزات جرمنوں کے ہاتھ لگوائیں، جس سے وہ غلط سمت میں فوجی تیاری کرنے لگے، ایک حقیقی ٹروجن طرز کا فریب تھا۔

یہ تمام واقعات اس بات کا ثبوت ہیں کہ ٹروجن ہارس کی حکمتِ عملی دراصل غیر متوقع حملہ، فریب، دھوکا، اور اعتماد کے غلط استعمال پر مبنی ہے جو آج بھی مؤثر ہے۔

جدید متوازی مثالیں: جاسوسی، خفیہ معلومات اور ہائبرڈ جنگ:

جدید دور میں ٹروجن اصول کی واضح جھلک ہائبریڈ جنگ (Hybrid Warfare) میں دیکھی جاسکتی ہے۔ یہ وہ جنگ ہے جو صرف روایتی ہتھیاروں سے نہیں لڑی جاتی بلکہ سائبر حملوں(Cyber Attacks) ، غلط معلومات کی اشاعت(Disinformation)، پروپیگنڈا(Propaganda) ، معاشی تخریب کاری (Economic Sabotage)، جیسے جدید اور غیر روایتی ہتھکنڈوں کے ذریعے لڑی جاتی ہے۔

• سائبر جاسوسی :(Cyber Espionage) دشمن ملک کے ڈیجیٹل سسٹمز میں ٹروجن سافٹ ویئر ذریعے خفیہ طور پر داخل ہو کر حساس معلومات، سرکاری ڈیٹا، اور سیکیورٹی ریکارڈ چرانا، یہ جدید دور کی خاموش مگر نہایت مؤثر جاسوسی حکمتِ عملی شمار ہوتی ہے۔ جیسے کہ Kiltz, Stefan, Andreas Lang, and Jana Dittmann لکھتے ہیں:

> The Trojan horse can be used in cyber-warfare and cyber-terrorism, as recent attacks in the field of industrial espionage have shown. (4)

•پروپیگنڈا مشینیں :(Propaganda Machines) سوشل میڈیا پلیٹ فارمز، ڈیجیٹل نیٹ ورکس اور آن لائن بوٹس کے ذریعے دشمن ملک کی عوامی رائے کو مؤثر طور پر منحرف یا تبدیل کرنا، غلط معلومات پھیلانا، اور سماجی انتشار پیدا کرنا جدید دور کی ایک اہم اطلاعاتی ٹروجن حکمتِ عملی تصور ہوتی ہے۔

•سفارتی ٹروجن ازم :(Diplomatic Trojanism) بظاہر سفارتی تعاون، تجارت، یا ترقیاتی شراکت داری کا تاثر دینا، مگر دراصل دشمن ملک کے پالیسی ڈھانچے میں خاموشی سے اسٹریٹجک دراندازی (Strategic Infiltration) کرنا یہ بین الاقوامی تعلقات میں ٹروجن ہارس اصول کی جدید اور نہایت باریک صورت ہے۔

مثلاً روس اور یوکرین کے تنازع میں سائبر ٹروجن (Cyber Trojan) اور اطلاعاتی جنگ (Information Warfare) کو ایک اہم ہتھیار کے طور پر استعمال کیا گیا۔ اسی طرح چین اور امریکہ کے درمیان مصنوعی ذہانت پر مبنی نگرانی (AI-based Surveillance) اور ڈیٹا جاسوسی (Data Espionage) بھی ٹروجن فلسفے (Trojan Philosophy) کی جدید اور پیچیدہ شکلیں ہیں۔

اخلاقی اور عالمی سلامتی کے مضمرات:

ٹرائجن اصول اگرچہ حکمتِ عملی کے طور پر مؤثر ہے، مگر اس کے استعمال سے اخلاقی حدود (Ethical Boundaries) اور عالمی سلامتی کے ڈھانچے (Global Security Frameworks) متاثر ہوتے ہیں۔ بین الاقوامی سطح پر، ٹروجن پر مبنی جاسوسی (Trojan-based Espionage) نہ صرف ریاستی خود مختاری (State Sovereignty) کے لیے ایک سنگین چیلنج بنتی ہے بلکہ ڈیجیٹل اعتماد (Digital Trust) کو بھی کمزور کرتی ہے، جو جدید عالمی نظام کا بنیادی ستون تصور ہوتا ہے۔

اسی باعث جدید فوجی ادارے اور انٹیلیجنس ایجنسیاں ''اخلاقی جنگی اصول (Ethical Warfare Doctrine)'' پر زور دیتی ہیں یعنی یہ کہ فریب (Deception) کو ایک جنگی حکمتِ عملی کے طور پر استعمال کیا جاسکتا ہے، لیکن شہری نظام (Civilian Systems) یا غیر جنگی مقامات (Non-Combat Zones) کو نشانہ بنانا نہ صرف غیر اخلاقی ہے بلکہ بین الاقوامی قانون (International Law) کی صریح خلاف ورزی بھی ہے۔

ڈیجیٹل دور کے لیے اسباق:

ٹروجن ہارس کی کہانی ہمیں ایک ایسے سبق سے روشناس کراتی ہے جو قدیم ٹرائے سے لے کر آج کے ڈیجیٹل معاشرے تک یکساں طور پر قابلِ اطلاق ہے: اعتماد قیمتی ہے، مگر اندھا اعتماد خطرناک۔

جدید دنیا میں جہاں تمام عناصر باہم جڑے ہوئے ہیں انسان، مشین، ادارے، اور ڈیٹا ، وہاں ٹرائجن کے اصول نے نئی معنویت اختیار کر لی ہے۔ یہ اب محض جنگی فریب (Warfare Deception) نہیں بلکہ ڈیجیٹل اخلاقیات، سائبر آگاہی، اور معلومات کی سالمیت (Information Integrity) کا بنیادی استعارہ بن چکا ہے۔

شک و تنقیدی سوچ کی اہمیت:

ڈیجیٹل عہد میں سب سے بڑی ضرورت تنقیدی سوچ (Critical Thinking) اور ڈیجیٹل خواندگی (Digital Literacy) کی ہے۔ صارفین کو یہ سمجھنا چاہیے کہ ہر آن لائن ذریعہ قابلِ اعتماد نہیں ہوتا، ہر ایپلیکیشن محفوظ نہیں، اور ہر پیغام محفوظ نہیں ہوتا۔ ٹروجن ہارس ہمیں یہ سبق دیتا ہے کہ فریب اکثر دوستانہ یا پرکشش چیز کے پیچھے چھپا ہوتا ہے۔ لہٰذا جدید تعلیم میں سائبر ہائجین (Cyber Hygiene) اور تحلیلی سوچ کو اسی اہمیت دی جانی چاہیے جس طرح ماضی میں خواندگی کو بنیادی اہمیت حاصل تھی۔

سوشل میڈیا کے دور میں غلط اور من گھڑت معلومات نئے ٹرائجن کے طور پر سامنے آئے ہیں۔ یہ ذہنوں کو متاثر کرتے ہیں، نظاموں کو نہیں انسانی فہم و شعور پر حملہ کرنے والی یہ معلوماتی جنگیں انہی ٹروجن حکمتِ عملیوں پر مبنی ہیں جن کا آغاز ٹرائے کے گھوڑے سے ہوا تھا۔

•ڈیپ فیک (Deepfakes) کے ذریعے جعلی بیانات یا ویڈیوز بنانا۔

•فشنگ لنکس (Phishing Links) کے ذریعے عوام کو data فراہم کرنے پر مجبور کرنا۔

•الگوریتھمک تعصب (Algorithmic Biases) کے ذریعے سیاسی یا سماجی رجحانات کو متاثر کرنا۔

یہ تمام مظاہر اس بات کی یاد دہانی کراتے ہیں کہ ٹروجن صرف ایک سافٹ ویئر نہیں بلکہ ایک نظامی حکمتِ عملی (Systemic Strategy) ہے۔ اس کا مؤثر مقابلہ صرف ٹیکنالوجی سے نہیں بلکہ آگاہی، تعلیم، اور اخلاقی ضابطہ کاری کے ذریعے ممکن ہے۔

ٹروجن ہارس آج کے دور کے لیے ایک فلسفیانہ انتباہ (Philosophical Warning) بھی ہے۔ یہ ہمیں یاد دلاتا ہے کہ انسانی فریب کی فطرت کبھی ختم نہیں ہوتی، یہ صرف اپنی شکل اور زریعہ بدلتی رہتی ہے۔ قدیم زمانے میں یہ فریب لکڑی کے گھوڑے میں چھپا ہوتا تھا، جبکہ آج یہ موبائل ایپلیکیشن، مصنوعی ذہانت کے نظام، اور سوشل نیٹ ورکس میں چھپا ہوا نظر آتا ہے۔ اس استعارے کا لازوال پیغام یہ ہے:

"Beware of gifts that come too easily, they may carry hidden costs."

ایسے تحائف سے محتاط رہیں جو بہت آسانی سے مل جائیں، ان کے پیچھے پوشیدہ خطرات یا قیمت یا اخراجات ہو سکتے ہیں۔

پوشیدہ خطرات سے ہوشیار رہنے کا پیغام:

ڈیجیٹل دور میں ٹرائجن صرف ایک تکنیکی خطرہ نہیں بلکہ ایک ثقافتی ذہنیت (Cultural Mindset) بن چکا ہے۔ لہٰذا جدید انسان کو درج ذیل اصول اپنانا ہوں گے:

- اندھا اعتماد کے بجائے باخبر اعتماد۔
- سہولت کے بجائے حفاظت اولین ترجیح۔
- تجسس کے بجائے احتیاط

یوں ٹروجن ہارس آج بھی ہمیں یہی سبق دیتا ہے کہ تحفظ اعتماد میں نہیں، احتیاط میں ہے۔

نتیجہ:

ٹروجن ہارس کی داستان، چاہے اسے ایک اسطوری کہانی سمجھا جائے یا انسانی فریب کی علامت، اپنے اندر ایک لازوال پیغام رکھتی ہے جو صدیوں سے انسان کو مخاطب کر رہا ہے۔ قدیم یونان کے کاریگروں نے ایک لکڑی کا گھوڑا بنا کر ٹرائے کے قلعے میں فریب سے داخلہ حاصل کیا، جبکہ جدید ہیکرز سافٹ ویئر ٹروجنز کے ذریعے ڈیجیٹل قلعوں کو توڑتے ہیں۔ دونوں میں مشترک بات ہے اعتماد کا استحصال ہے۔

قدیم اساطیر سے جدید دور تک اہم نکات کا خلاصہ

- ٹروجن ہارس محض ایک جنگی کہانی نہیں بلکہ انسانی ذہانت اور فریب کی نفسیاتی داستان ہے۔
- یہ تصور وقت کے ساتھ سیاسی، معاشی، عسکری، اور تکنیکی دائرے میں منتقل ہوا۔
- سائبر سیکیورٹی کے میدان میں یہ سب سے نمایاں علامت ہے کہ دشمن ہمیشہ باہر سے نہیں، اکثر اندر سے وار کرتا ہے۔

•ڈیجیٹل دنیا میں ٹرائجن کی علامت ہمیں معلوماتی جنگوں، جعلی خبروں، اور مصنوعی ذہانت پر مبنی اثر ورسوخ کے خطرات سے خبردار کرتی ہے۔

انسانی تاریخ یہ ثابت کرتی ہے کہ فریب انسان کی بنیادی جبلتوں میں سے ایک ہے۔ یہ کبھی مٹ نہیں سکتی، صرف مہذب شکل اختیار کر لیتی ہے۔ اسی لیے ٹروجن ہارس محض ماضی کی علامت نہیں بلکہ مستقبل کی تنبیہ بھی ہے۔ جب تک انسان تجسس، لالچ، یا اندھا اعتماد کے تابع رہے گا، ٹرائجن کسی نہ کسی صورت میں زندہ رہے گا-چاہے وہ لکڑی کے گھوڑے کی شکل میں ہو، یا کسی معصوم دکھنے والی موبائل ایپ کی صورت میں۔

ٹروجن ہارس آج بھی زندہ ہے، ڈیجیٹل روپ میں

ٹروجن ہارس دراصل ایک لازوال استعارہ ہے۔ یہ ہمیں یاد دلاتا ہے کہ طاقت صرف ہتھیاروں سے نہیں، بلکہ ذہانت، فریب، اور بصیرت سے حاصل ہوتی ہے۔ اور جدید دنیا میں، جہاں ڈیٹا ہی نیا خزانہ ہے، ٹروجن ہارس ہر اس خطرے کی نمائندگی کرتا ہے جو اعتماد کے پردے میں چھپا ہو۔

The Trojan Horse lives on – not in the walls of Troy, but in the codes of our digital world.

یہ گھوڑا آج بھی زندہ ہے، مگر اب لکڑی کا نہیں، ڈیجیٹل ہے۔

حوالہ جات

1. Murphy, Lauren. "Horses, Ships, and Earthquakes: The Trojan Horse in Myth and Art." Iris Journal of the Classical Association of Victoria (New Series) 30 (2017): 18-37.

2. Gozzi, Raymond. "The Trojan horse metaphor." ETC: A Review of General Semantics 57.1 (2000): 80-84.

3.Meyerson, Bruce. (June 15, 1999) "Worm Digs Deeper in Networks." Ithaca (New York) Journal , 6 A

4.Kiltz, Stefan, Andreas Lang, and Jana Dittmann. "Malware: specialized trojan horse." Cyber Warfare and Cyber Terrorism. IGI Global Scientific Publishing, 2007. 154-160.